Exhibit B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS, VERIZON CORPORATE SERVICES GROUP INC.,
T-MOBILE USA, INC.,
AT&T SERVICES, INC., AT&T MOBILITY LLC, AND AT&T CORP.
Petitioners,

v.

HEADWATER PARTNERS I LLC.
Patent Owner.

U.S. Patent No. 9,198,042
Title: SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

Inter Partes Review No.: IPR2024-00809

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,198,042 UNDER 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-.80, 42.100-.107

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

Petitioner's Exhibit List

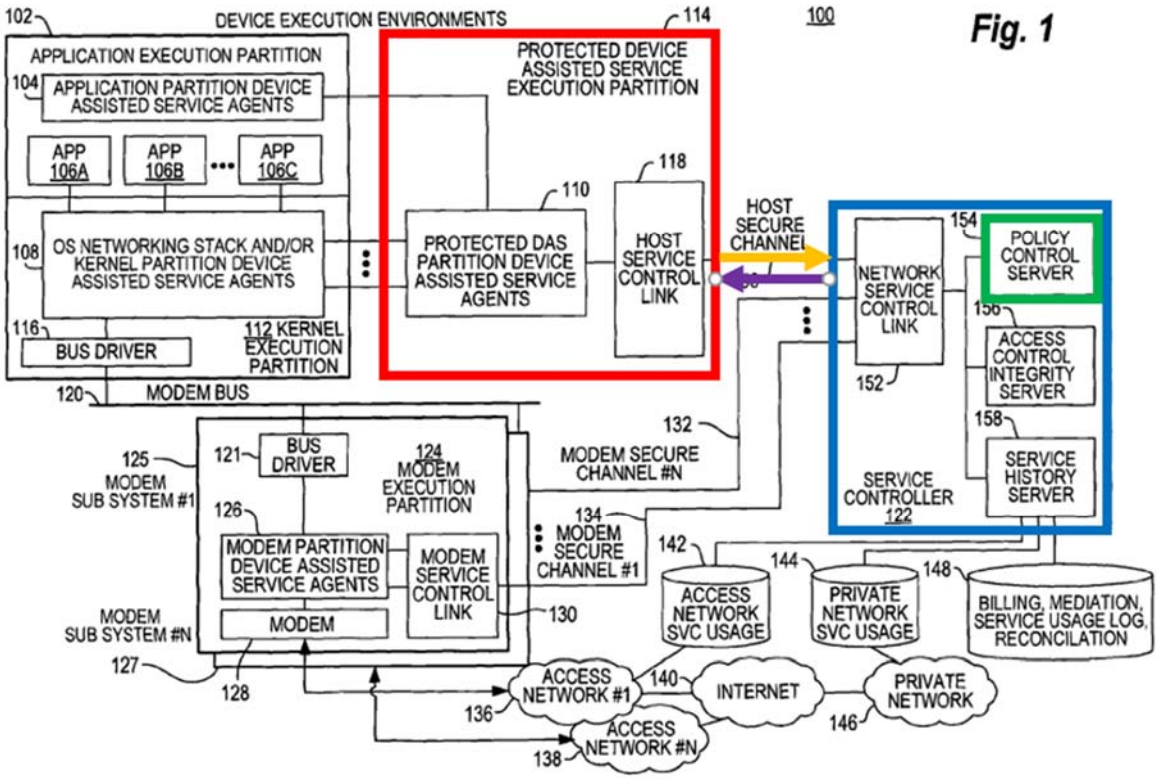
Exhibit #	*Description*
1001	U.S. Patent No. 9,198,042 ("the '042")
1002	Prosecution history of the '042 ("'042 File History")
1003	Declaration of Petitioner's Expert Petitioners expert, Dr. Henry Houh
1004	U.S. Publication No. 2007/0006289 ("Limont")
1005	U.S. Publication No. 2004/0123153 ("Wright")
1006	U.S. Publication No. 2006/0183461 ("Pearce")
1007	U.S. Publication No. 2007/0288989 ("Aarnos")
1008	U.S. Publication No. 2007/0104169 ("Polson")
1009	Arm TrustZone Microprocessor Report
1010	Arm TrustZone Paper
1011	U.S. Publication No. 2006/0112427
1012	U.S. Pat. No. 7,849,310
1013	Limont Prosecution History Excerpts (Application No. 11/171,850)
1014	U.S. Publication No. 2006/022474A1
1015	U.S. Publication No. 2009/0265754
1016	U.S. Publication No. 2007/0061535 ("Xu")
1017	U.S. Pat. No. 8,064,417
1018	U.S. Pat. No. 7,672,695
1019	U.S. Pat. No. 7,881,267
1020	U.S. Publication No. 2008/0244018
1021	Plaintiff's Infringement Contention (Verizon case)
1022	Docket Control Order
1023	List of Related Applications

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311 *et seq*. and 37 C.F.R. §§ 42.1 *et seq*., Cellco Partnership d/b/a Verizon Wireless, Verizon Corporate Services Group Inc., T-Mobile USA, Inc., AT&T Services, Inc., AT&T Mobility LLC, and AT&T Corp. (collectively, "Petitioners") hereby petition for an *inter partes* review of U.S. Patent No. 9,198,042 ("the '042 Patent") (EX-1001). Petitioners respectfully submit that Claims 1-18 (the "Challenged Claims") of the '042 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioners will prevail on at least one Challenged Claim. Accordingly, Petitioners respectfully request that the Board institute an *inter partes* review of the '042 Patent pursuant to 37 C.F.R. § 42.108.

II. OVERVIEW

The Challenged Claims are unpatentable as obvious over the prior art. The claims are directed to prior art methods for: (1) receiving information from a wireless device regarding the current service policy that controls the device's ability to access a network data service; and (2) reconfiguring the wireless device based on that information. The architecture for performing the method is shown in FIG. 1 of '042 Patent:



EX-1001, FIG. 1.[1]

A **service controller (blue)** receives, over a **service control link (gold)**, a report from a wireless end-user device containing information about the service policy settings of the **mobile device (red)**. The server controller determines whether the current service policy setting of the wireless end-user device needs to be modified to allow the wireless device to access a network data service. The service policy setting is stored in a protected partition (red) of the wireless end-user device to deter or prevent unauthorized modifications to the particular service

[1] Unless otherwise noted, all annotations and emphases herein are added.

policy setting. If the service policy setting needs to be modified, the **server sends (purple)** new **policy settings (green)** to the wireless device. The protected partition can be provided by encrypting the policy settings on the wireless device.

U.S. Publication No. 2007/0006289 ("Limont") (EX-1004) is a parallel disclosure to the '042 Patent—it discloses the architecture and the same claimed method as the '042 Patent, but uses different language. Limont's FIG. 3 discloses the same architecture for performing the claimed method, using color coding to identify components in common with the '042 Patent:

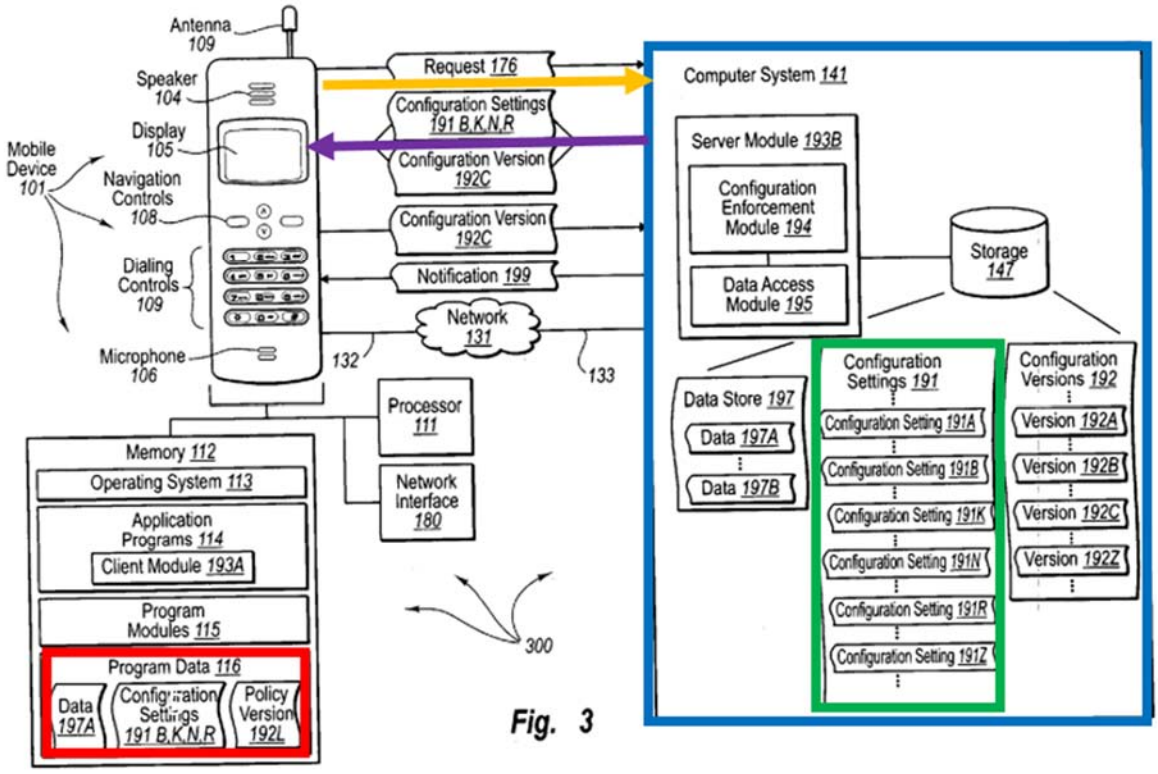


Fig. 3

EX-1004 FIG. 3.

A **computer system (blue)** receives, over a **service control link (gold)**, a report from a wireless end-user device containing information about the policy settings of the **mobile device (red)**. The server controller determines whether the current service policy setting of the wireless end-user device needs to be modified to allow the wireless device to access a network data service. If the service policy setting needs to be modified, the **server sends (purple)** new **policy settings (green)** to the wireless device. Limont states policy settings should be "locked down" on the wireless device, but does not expressly state that the policy settings should be encrypted. Wright (EX-1005) and Xu (EX-1016) disclose that policy settings should be encrypted (and optionally stored in secure memory) on a wireless device in order to prevent unauthorized access to the settings.

Thus, the proposed combination is directed to the same problem as the '042 Patent and proposes the same solution. Thus, the Challenged Claims are unpatentable over this combination. EX-1003, ¶¶258-695.

III. GROUNDS FOR STANDING (37 C.F.R. § 42.104(A))

Petitioners certify that the '042 Patent is available for, and that Petitioners are not barred or estopped from requesting, a post grant review of the Challenged Claims on the grounds herein. 37 C.F.R. § 42.104(a). This Petition is filed pursuant to 37 C.F.R. § 42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in §§ II and VI-VIII of this Petition and in the attached Declaration of Petitioners' Expert, (Henry Houh) (EX-1003), the method of modifying the service policy settings of a wireless device as claimed in the '042 Patent, is obvious over the prior art to a person of ordinary skill in the art ("POSA") at the priority date.

IV. BACKGROUND

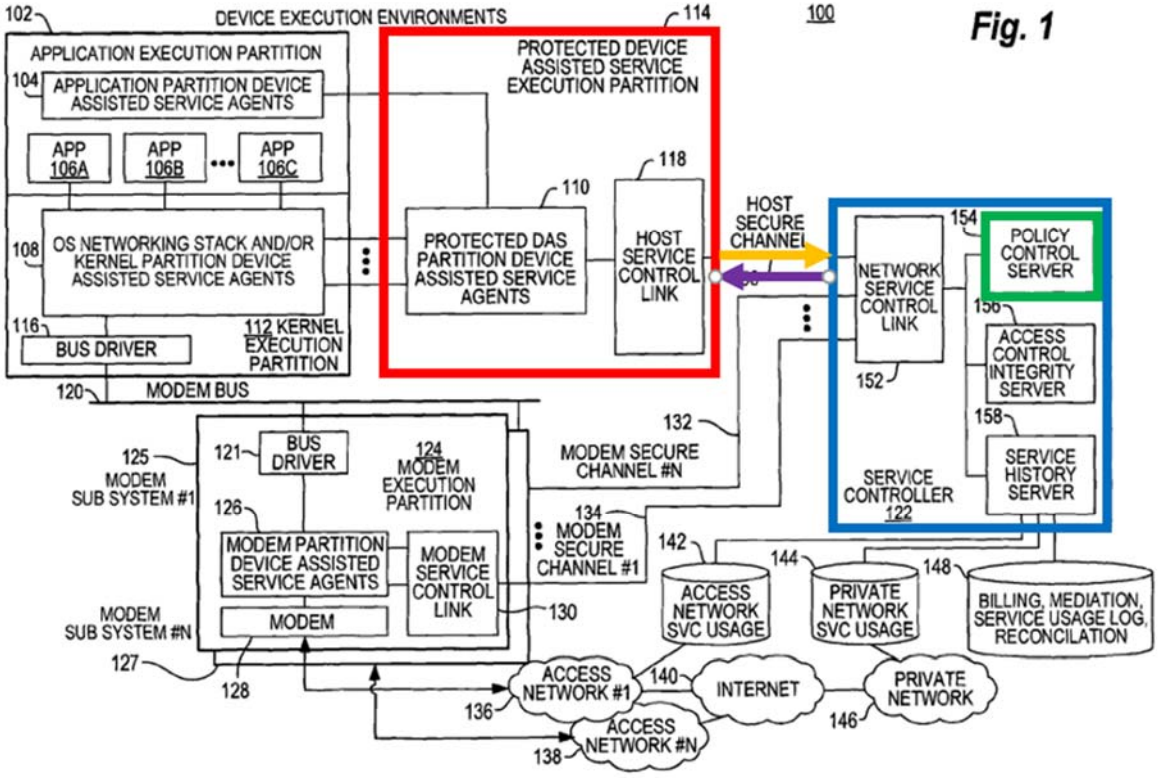
A. Summary of the '042 Patent

The '042 Patent describes a method of reconfiguring a wireless device based on information received from a wireless device regarding the service state of the device. EX-1001, Abstract. The service state of the device is provided by reports from the device, or derived outside the device, and can include various data. EX-1001, 13:56-14:11; 18:6-11; Claims 14-18.

In the '042 Patent, a service controller receives the reported information and determines that a particular service policy setting that provides for access to a network data service needs to be modified. The service policy setting is stored in a protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting. The service controller, in response to determining that the particular service policy setting needs to be modified, sends configuration

information to the wireless device to assist in modifying or allowing modifications to the particular service policy setting. EX-1001, Abstract.

FIG. 1 of the '042 Patent depicts an embodiment for reconfiguring device.



EX-1001, FIG. 1.

Protected device assisted service ("DAS") agents, execute in the protected DAS partition (red). The protected DAS partition can make it more difficult for an unauthorized entity to modify the device's confidential data. EX-1001, 6:23-37.

The '042 Patent describes that in some embodiments, the protected DAS partition prevents other elements on the device from writing and/or reading certain memory areas reserved for device assisted service agents and/or control link

functions. This can be accomplished by encrypting traffic to and from memory so that only authorized device program elements possess the counterpart encryption capability to access the memory. EX-1001, 9:17-36. The '042 Patent describes that policy server (green) stores policy settings that can be implemented on the device, and communicates appropriate policy settings to the device. EX-1001, 8:26-30.

B. Prosecution History

Claims 1-18 received a first Office Action allowance with no prior art applied. The Examiner merely stated "the prior art, either alone or in combination, does not disclose Applicant's inventive claim language." EX-1002, 000048.

C. Claim Construction

Petitioners propose that each claim term in the Challenged Claims be given its plain and ordinary meaning in this proceeding, because the prior art relied on in this Petition meets each claim term under any reasonable construction.

D. Priority Date

The '042 Patent's application claims priority to various applications, the earliest of which was filed January 28, 2009. The prior art cited below predates this date.

E. Person of Ordinary Skill in the Art

A POSA at the time of the invention would have been familiar with the changing of configuration settings of end-user devices to control access of the

device to network data services, and storing those configuration settings in a protected partition. A POSA would have gained this knowledge through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and two years of experience. EX-1003, ¶¶41-43.

F. State of the Art

The following section describes the state of the art for storing, modifying and protecting a mobile device's policy settings as of January 2009. EX-1003, ¶¶144-255. The references, and knowledge of a POSA, provide the factual support for additional motivation to modify or combine the references. Accordingly, these references should be considered by the Board.

1. Mobile Phone Policy Settings

It was known to use policy settings stored on a wireless device to control the wireless device including providing access to data networks, the type of communications permitted, the type of communication protocol used, the use of communications applications, and the identification of the wireless carrier. For example, one prior art system teaches modifying policy settings in a wireless device that may roam between regions. A server transmits policies which determine through which networks mobile device can access. EX-1006, Abstract.

The device maintains a database of the communication policies. EX-1006, [0040]. The policies provide differential access in different regions, or based on

cost or type of linkage. EX-1006, [0009-0014]. The policy allow specific service access for voice calls, web browsing, e-mails, etc. EX-1006, [0060].

2. Modifying Stored Policies on Mobile Phones

It was known that policies could be stored on a mobile phone and subsequently modified. For example, before a stored policy could be modified, an electronic signature or key is verified to determine if the modification is authorized. EX-1007, [0025]. This verification process is also used to provide different levels of authorization. EX-1007, [0023].

3. Protected Partitions

Providing protected partitions of memory that restricted access to critical data was well-known and pervasive in mobile devices by the 2009 priority date. Schemes for protecting memory included both hardware controls and encryption. For example, Arm's "TrustZone" technology was patented starting in 2003. EX-1009, EX-1010, EX-1012. In such systems, [t]he memory protection unit is managed by the secure operating system … defining the partitions between the secure memory and the non-secure memory." EX-1012, 39:64-67, 37:23-50:17. Similarly, it was known to "encrypt" or "hide" confidential data on mobile devices. *E.g.*, Section VI.A.2

A POSA at the time of the invention would have known from the prior art that critical data, such as policies, would be beneficially stored in protected

(encrypted) memory partitions to prevent unauthorized access. U.S. 2006/0112427((EX-1011), [0005-0006], [0060]; U.S. 2006/0224742A1 (EX-1014), [0127-0128] U.S. 2009/00265754 (EX-1015) [0052-0055].

V. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

This Petition challenges claims 1-18 of the '042 Patent.

B. Statutory Grounds for Challenges

The Challenges are set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	1-2, 6-18	§ 103	Limont in view of Wright and optionally in further view of Xu
2	3-5	§ 103	Limont in view of Wright and optionally Xu in further view of Polson

Ground 1: Claims 1-2, 6-18 of the '042 Patent are obvious over Limont in view of Wright and optionally Xu.

U.S. Patent Publication No. 2007/0006289 published on January 4, 2007 from an application filed on June 30, 2005 ("Limont") (EX-1004). Limont is prior art under §102(a)(b)(e)(g).

U.S. Patent Publication No. 2004/0123153 published on June 24, 2004 from an application filed on April 11, 2003 ("Wright") (EX-1005). Wright is prior art under §102(a)(b)(e)(g).

U.S. Patent Publication No. 2007/0061535 published on March 15, 2007 from an application filed on September 12, 2005 ("Xu") (EX-1016). Xu is prior art under §102(a)(b)(e)(g).

Ground 2: Claims 3-5 are obvious over Limont in view of Wright, and optionally Xu, in further view of Polson.

U.S. Patent Publication No. 2007/0104169 published on March 10, 2007 ("Polson") (EX-1008). Polson is prior art under §102(a)(b)(e)(g).

VI. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-2, 6-18 are obvious over Limont in view of Wright and optionally Xu.

Limont, Wright and Xu are devoted to updating and securing policies on mobile devices. Limont provides the primary invalidating disclosure with the structure and functionality corresponding to the Challenged Claims. Wright provides aspects of the claims related to *a protected partition* by disclosing the use of encryption of policy settings in memory. Xu provides another example of a *protected partition* using a hardware-enforced protected memory partition.

1. Limont

Like the '042 Patent, Limont teaches configuring and updating policy settings for a wireless device based on information received from that device regarding the service state of the device. FIG. 3 illustrates an architecture for configuring and updating policy settings:

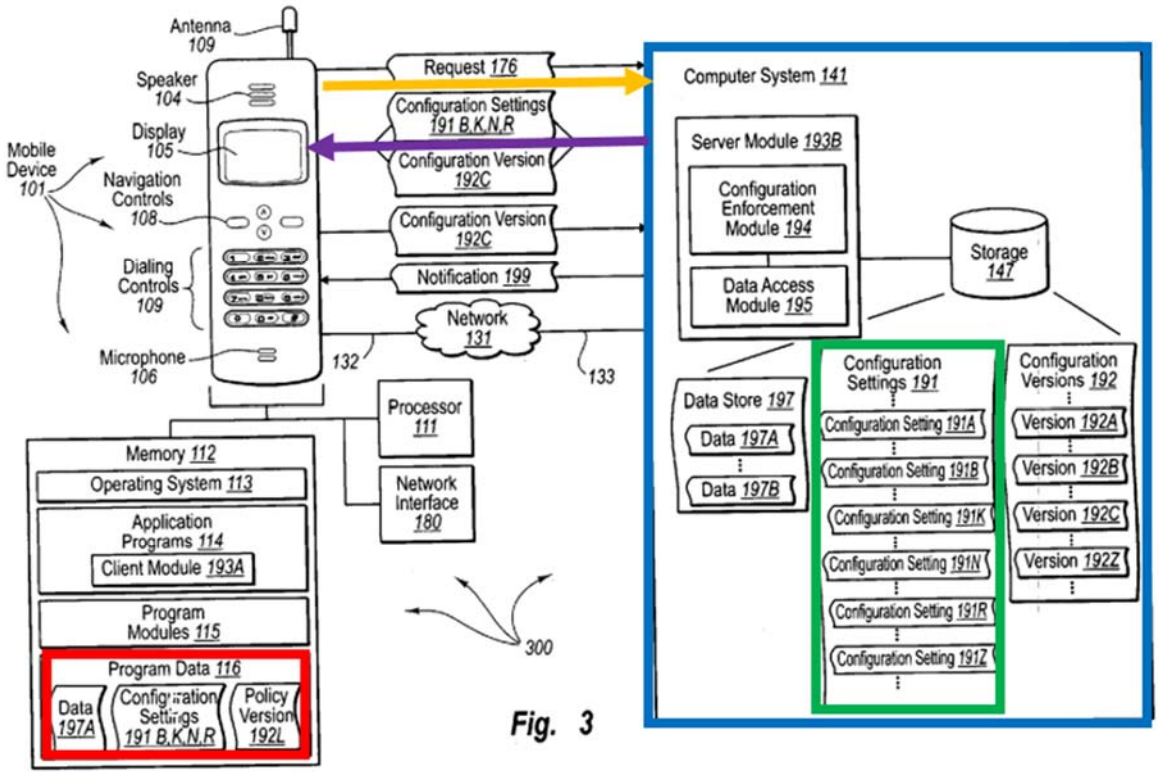


Fig. 3

EX-1004 FIG. 3. EX-1003 ¶¶54-56. Mobile device 101 may include client module 193A (*e.g.*, a Web browser) to access data maintained by server module 193B. The server includes policy enforcement module 194 and data access module 195. EX-1004, [0073]. EX-1003 ¶¶59-60.

Server module 193B interoperates with client programs (*e.g.*, client module 193A) to transfer data (*e.g.*, Web pages) to mobile device 101. Thus, in response to a mobile device data request for access to the web server, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data. For example, policy enforcement module 194 can determine if sufficient resources have allocated at a mobile device to receive a

Web page, if a mobile device Web browser includes correct plug-ins for viewing content, if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time, etc. EX-1004, [0077]; EX-1003 ¶¶61-63.

Configuration enforcement module 194 (in addition to user authentication and authorization modules) checks the device's configuration / policy settings and allowing access module 195 to access and either transfer the requested data or updated configuration settings (policies) to allow for such access. EX-1004, [0078], Abstract. Limont references the "configuration enforcement module" as "policy enforcement module" and "configuration settings" as "policy settings." EX-1004, [0077], [0083], [0055]; EX-1003 ¶64.

Limont's FIG. 4 illustrates a flow chart of a method for enforcing an appropriate mobile device configuration using the architecture of FIG. 3:

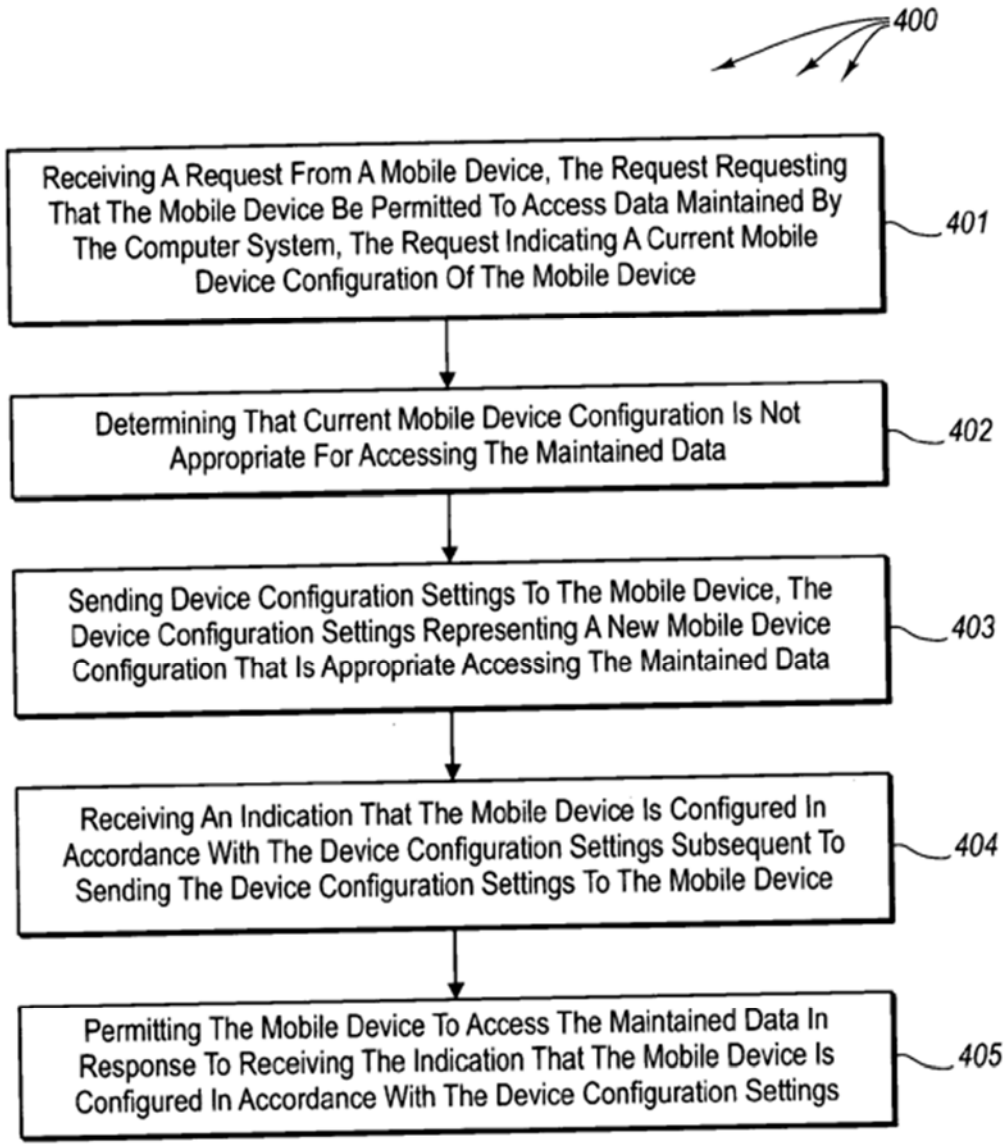


Fig. 4

EX-1004 FIG. 4; EX-1003 ¶¶65-66.

Using the architecture shown in Limont's FIG. 3, method 400 in Fig. 4 shows the claimed updating of policies.

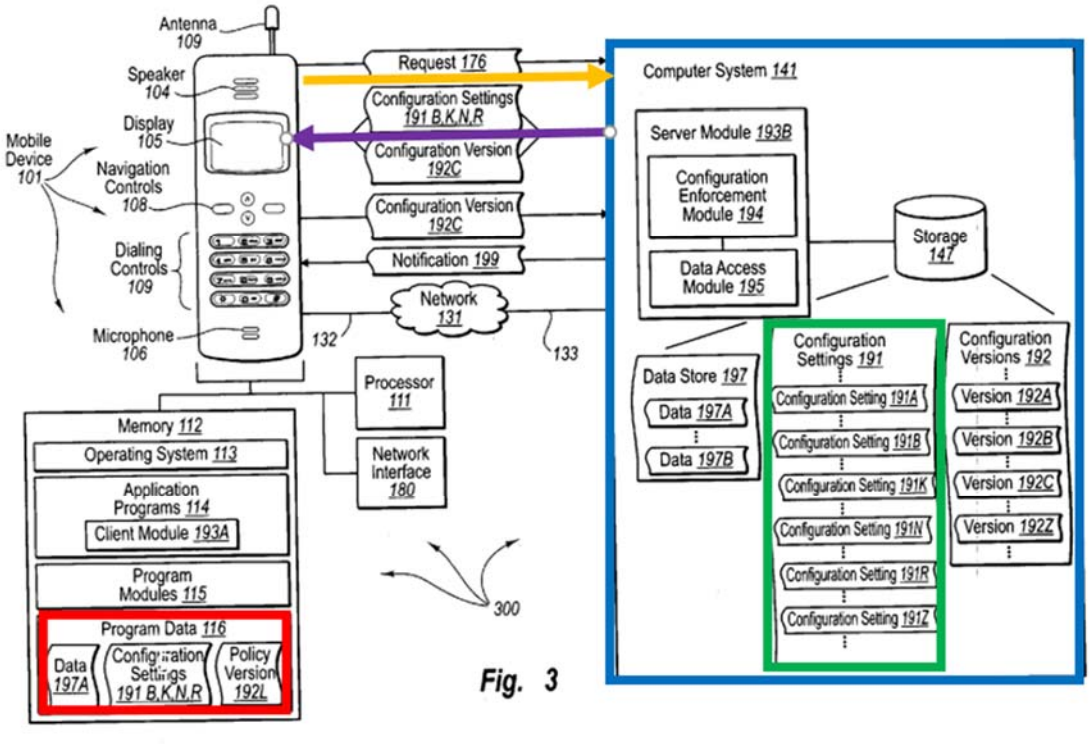


Fig. 3

EX-1004 FIG. 3; EX-1003 ¶67.

In step 401, the mobile device sends request 176. Request 176 can include: (1) a current configuration version of the mobile device 101; (2) a data request, such as for a Web page; and/or (3) an express request for new configuration settings. EX-1004, [0080]. Configuration settings can include policy settings, operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc. EX-1004, [0073]; EX-1003 ¶68.

In step 402 (202), configuration enforcement module 193 determines whether the configuration setting in the request is appropriate to access the

requested data. If so, then the data can be accessed. EX-1004, [0081-0082], [0070]; EX-1003 ¶69.

If the device's configuration setting is "inappropriate" for the data access, then the server sends modified settings to the mobile device (step 403/206). EX-1004, [0083]. For example, server module 193B can send configuration settings 191B, K, N, and R along with configuration version 192L to mobile device 101 in response to request 176 (a request). EX-1004, [0084]. Mobile device 101 can store implement configuration settings 191B, K, N, and R (potentially altering current configuration settings) to comply with configuration settings that are appropriate for accessing data maintained by server module 193B. EX-1004, [0086]; EX-1003 ¶70.

In step 405, the computer system 141 permits the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device configuration settings. EX-1004 [0089]; EX-1003 ¶71.

2. Wright

Wright teaches protecting data on mobile computing devices using various security tools. Wright explains that data stored on a mobile device is vulnerable to hackers even if that data was transmitted from a server using a secure trusted connection, such as a VPN. EX-1005, [0007-0009]; EX-1003 ¶¶73.

Wright stores configuration information on a mobile device including the current version of the security policy software components for the mobile device, the current policy settings on the device, and attributes in accordance with those settings, for example, which ports are blocked. EX-1005, [0057]; EX-1003 ¶82. Wright explains that one solution to the security issue identified above is to maintain the policy documents as XML documents to allow great flexibility in design, usage, and enhancement of policies. Using the flexibility of XML policy documents simplifies the complex problem of distributing and enforcing policies directed to program usage, network access, hardware restrictions, VPN access, data access, and many other policies. Wright explains that the policies can be protected from hacking by encryption or signatures (*i.e.*, XKMS, XMLDSIG, XMLENC, or proprietary encryptions). The policy is then enforced on the client by a process that can interpret the policy distributed by the enterprise. This approach allows a policy to be extensible and easily updated by the administrator. Also, the administrator can configure elements of the policy such that they are configurable by the user. EX-1005, [0270]; EX-1003 ¶84.

Wright's computer system acts as a server for a client mobile device. The server includes a policy management module that sets the permissions for the mobile device regarding the policies. Permissions typically relate to the allowable modification that may be made to a downloaded policy or software. EX-1005,

[0078-0103]; EX-1003 ¶85. For example, the policy management module determines whether the security information is to be encrypted. If it is to be encrypted, the policy is encrypted. Security policies may be included in XML documents which may themselves be encrypted. EX-1005, [0104]; EX-1003 ¶86. Furthermore, files stored on the mobile device may be encrypted. EX-1005 Abstract, [0177], [0260]; EX-1003 ¶¶87-89.

Wright also describes using a secure trusted channel to provide the security policy for the server to the mobile device. A server's distribution module determines if the security policy has been designated to be encrypted. If so, then the security information is encrypted and distributed to the mobile device. EX-1005, [0128], [0267], Fig. 3A (elements 311, 312), Fig. 3C; EX-1003 ¶¶90-94.

Wright also discloses a client diagnostics module that audits files, including the security policy to verify no corruption (*e.g.* checksum). EX-1005, [0068-0073]. A server's remote diagnostics module receives audit logs from a client and analyzes the audit information to check the integrity of the stored files. The remote diagnostic module may provide a repair to a problem in the client device, determine that a trend is occurring for the device, or determine that preventive maintenance is to be scheduled for the client device. EX-1005, [0055]; EX-1003 ¶95.

3. Xu

Xu provides a protected partition of the mobile device's processor for storing and enforcing policies and encryption that matches the "protected partition" disclosed in the '042 Patent. EX-1003 ¶¶97-118. Xu is detailed below in element [1.3].

4. Motivation to Combine Limont's Teachings with Wright's Teachings and Optionally Xu's.

A POSA would be motivated to combine Limont with Wright and optionally Xu with a reasonable expectation of success. EX-1003, ¶¶263-298, ¶¶427-440, ¶¶165-222.

A POSA would recognize that the three references teach the same subject of managing and updating secure data, including policies, wirelessly on mobile devices. Limont and Wright have overlapping and complementary identification of problems (administrators managing policies on devices for traveling corporate users) and proposed solutions (wireless updates). EX-1003, ¶¶264-267. A POSA would have been motivated to consider, and combine, references from leading companies (Microsoft and Apple), describing the same technology, and identify the same problem addressed by their disclosures. EX-1003, ¶¶267.

Reflecting this heavy overlap, Limont's Examiner cited Wright repeatedly in Limont's prosecution. EX-1013, 0000140-141, 000145-146. Limont's Examiner held that Wright disclosed Limont's steps 401, 402, and 201 – which are relied

upon below for invalidity. EX-1013, 000147-148, 229-000230. The Examiner's citations: (1) demonstrate that a POSA (examiner) considered the references as closely related; and (2) would have identified to a POSA a set of references to consider. EX-1003, ¶¶268-277.

Limont and Wright both: (1) identify data security as a critical issue; (2) identify a problem arising from traveling users seeking to use wireless technologies to access data for flexible access from many locations; and (3) identify a separate problem from "hackers" or "malicious" entities physically accessing lost or stolen devices. EX-1003, ¶¶278-287 (citing and comparing EX-1004, [0004-0015] with EX-1005, [0005-0010]). For example, Limont identifies that an "increased risk of loss or theft" of mobile devices which "hackers" may use to access secure data. EX-1004, [0013]. Correspondingly, Wright notes that "hackers in the parking lot could break into the remote device and copy or maliciously alter the data." EX-1005, [0009]. Moreover, because policies on the device stored confidential credentials used for remote access, such as encryption algorithms, keys, and the user's password and PIN, a POSA would have further recognized that such policy information needed be protected on the mobile devices or "locked down." EX-1003, ¶¶283-287.

Thus, a POSA would have recognized that it was important to: (1) secure the confidential data (policy updates) during their wireless transmission; and (2)

prevent "malicious users" from accessing critical data on mobile devices if those devices were lost or stolen – both to protect the data on the device and to protect from "hackers" accessing credentials that would allow them to access data on corporate servers. EX-1003, ¶¶286-287. These are motivations to combine that come directly from both references. Thus, a POSA would have been motivated to combine Limont and Wright to provide an architecture that updates policies wirelessly and protects those updates both in transmission and on the end-user devices – thus addressing the specific problems (motivations) identified in both referenes. EX-1003, ¶¶288-291.

Limont provides the architecture for updating policies wirelessly (addressing one of the common problems for traveling users) and identifies that "encryption algorithms" and "keys" are available on mobile devices to use for wired access. However, Limont does not expressly provide protection for data on the device. Wright provides the complementary solutions of encrypting data during transmission and encrypting the data in the device's memory (as detailed below) that addresses the further problems identified by both references. EX-1003, ¶¶289-293.

Wright provides the other part of the solution. Wright discloses that the policy settings can be kept in a schema or document in XML format which can then be encrypted and sent to the mobile device and stored in encrypted form using

well-known encryption techniques. Thus, a POSA would have been motivated by the recognition that the combination of Limont and Wright addresses the problems identified in each. EX-1003, ¶¶289-293.

Furthermore, Limont and Wright identify complementary solutions for identifying and addressing potential malicious modifications. Wright discloses auditing the policy settings stored on the mobile device to determine the integrity of the data, *e.g.*, whether it has been corrupted (such as by the "malicious users" identified in Limont). Limont discloses that administrators may remotely "wipe" the device's data to protect that data. EX-1004, [0047-0049]. A POSA would have recognized that Wright's "audit" teaching provides the information for Limont's corporate administrators to effectuate their action (wipe) to protect the data. Limont's actions also fit squarely with Wright's teaching of attempts to "repair" any corrupted files as detailed below. EX-1003, ¶¶294, 283.

A POSA would be motivated to modify Limont's teachings of storing policy settings on the mobile device by encrypting the policy settings as taught by Wright. EX-1003, ¶¶293, 295. A POSA would be motivated to do so because unauthorized access to the data would: (1) allow a "malicious user" access to the device's policies (which may also permit hacker's remote access to corporate data); and (2) allow even an "authorized" user to change the policies (intentionally or

inadvertently) to access unauthorized networks, potentially avoid billing charges, and use unauthorized resources (*e.g.*, network bandwidth). EX-1003, ¶295.

A POSA would have a reasonable expectation of success as the modification is a software solution which uses known encryption techniques for their intended purpose ---securing the stored data. Limont already provides the hardware and software to implement encryption algorithms/keys. EX-1004, [0009], Fig.1 (processor 111, memory 112), [0040]. Using Wright's encryption techniques with Limont's system is merely the application of well-known operations (encrypting data), operating on known components (processors and encryption software), for their known and intended purposes (data protection). EX-1003, ¶¶296-297.

The detailed motivation to incorporate Xu and reasonable expectation of success is addressed in element [1.3]. Xu provides a complementary and supplementary mechanism for protecting policies both during wireless transmission and in the device's storage by using hardware-enforced protected memory. Thus, a POSA would have been motivated to consider Xu's supplementary solution for the same reasons as discussed above for Wright. ¶¶427-440, ¶¶165-222.

Furthermore, it was known in the art to protect confidential data, including policies, using protected partitions of memory implemented both using encryption

and/or with hardware-enforced techniques – providing a further motivation to combine. Section IV.F.3; EX-1003, ¶¶165-222.

5. Detailed Application to the Challenged Claims

a. Claim 1

[1.0] A method comprising:

Limont discloses a method for enforcing an appropriate mobile device configuration prior to permitting a mobile device to access maintained data, as shown in FIG. 4.

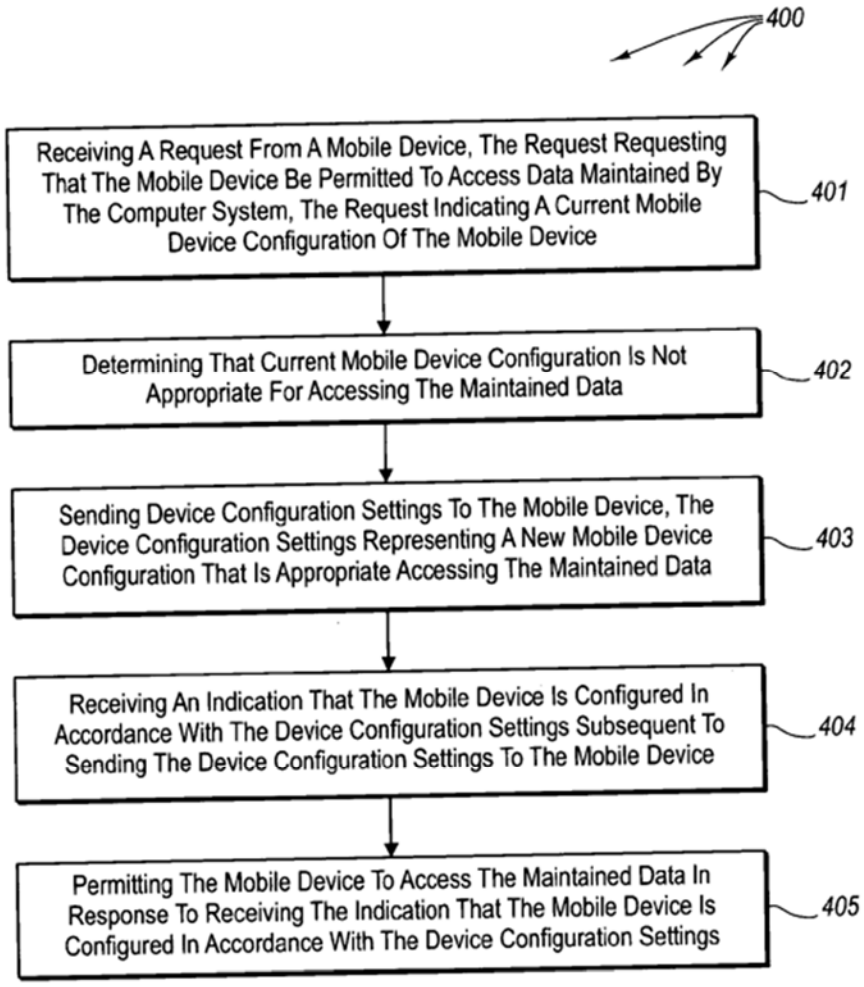


Fig. 4

EX-1004, FIG. 4.

Limont's FIG. 3 as annotated ("Annotated FIG. 3") illustrates an architecture for performing the method of FIG. 4:

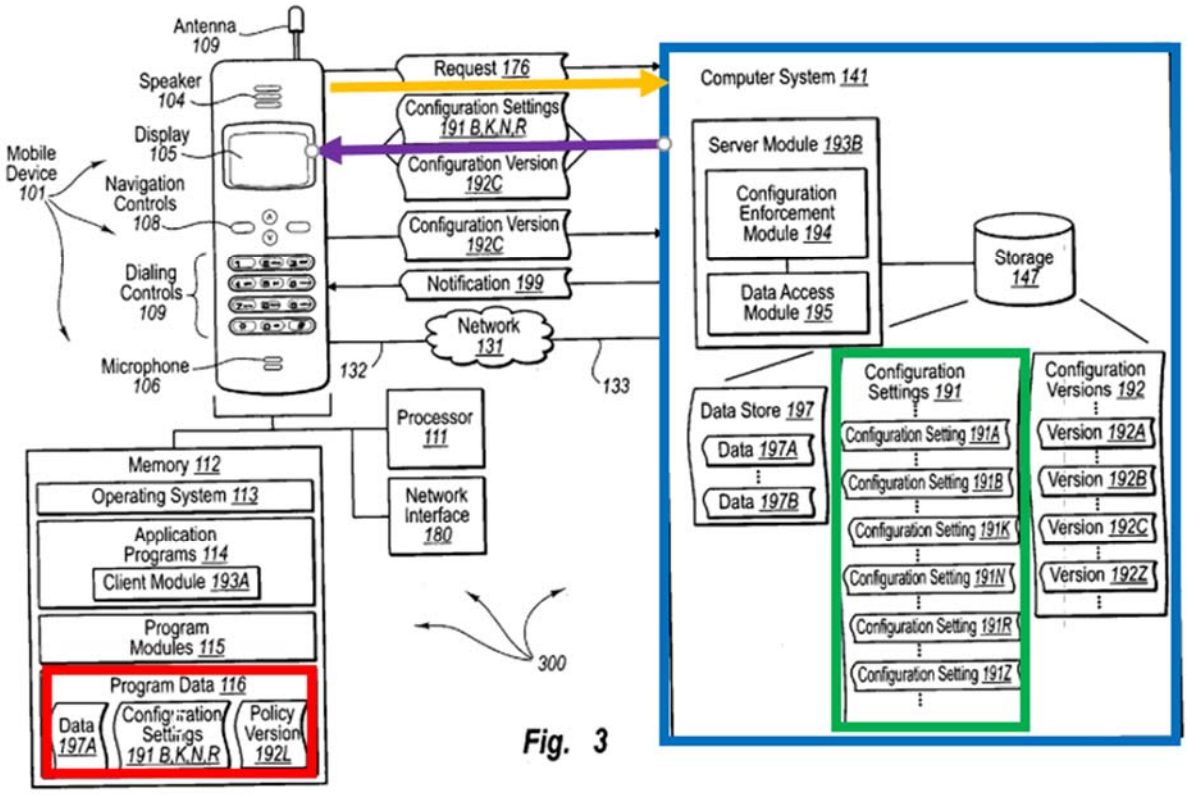


Fig. 3

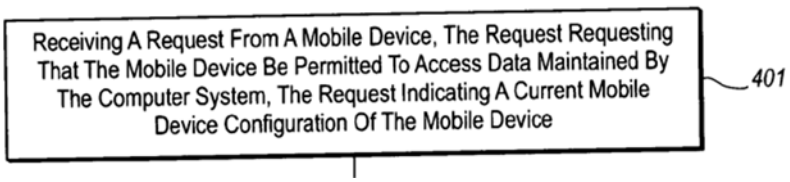
EX-1004 FIG. 3; EX-1003 ¶¶300-303. *See also* EX-1004, FIGs. 1, 2.

Limont's invalidating disclosure is presented primarily below using Figs. 3 and 4 (and their descriptions). However, Figs. 1 and 2 (and their descriptions) also contain parallel invalidating disclosure. Petitioners rely upon the corresponding disclosures in Figs. 1 and 2 (and their descriptions) for invalidity herein. EX-1003 ¶¶304-307.

[1.1] receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;

Limont discloses this limitation. EX-1003, ¶¶309-341. As illustrated in Annotated FIG. 3, Limont's computer system 141 (**blue**) receives request 176

(**gold**) from mobile device 101 (*receiving a report from a wireless end-user device*). The request (*report*) can include a configuration version representing one or more of the current configuration setting (*information about a device service state*) of mobile device 101 as in FIG. 4. EX-1004, [0080]-[0081].



EX-1004 FIG. 4, step 401. The "data command" in Fig. 2, step 201 and the "data request 164 / policy version 118D" are also reports with the same information corresponding to this element. EX-1004, [0030], [0055], [0058-0059], [0067-0069]. EX-1003, ¶¶314-327.

Limont's "configuration settings" include "policy settings … operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol setting, etc." EX-1004, [0073], [0047] (exemplary "policy settings"). Limont's disclosure of "configuration settings" and "policy settings" is consistent with the '042 Patent's disclosure that describes that device service state includes current service usage policy settings, current DAS settings, device status information, application status information, or other state and/or settings information. EX-1001, 17:46-18:11. EX-1003, ¶¶315-327. Therefore because the received "configuration version" /

"policy version" are "information about" Limont's mobile devices' "configuration settings" / "policy settings," they are "*information about the device service state*." EX-1003, ¶¶328-331.

Limont's communication links 132, 133 in FIGs. 1 and 3 (*a service control link*) allow Limont's wireless end-user device to communicate with the computer system. EX-1004, [0038]. Communication links 132 and 133 include using one or more different wireless protocols (e.g., GPRS, GSM, etc.) *over a wireless access network*. EX-1004, [0043], [0056]. EX-1003, ¶¶332-341.

[1.2] determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified,

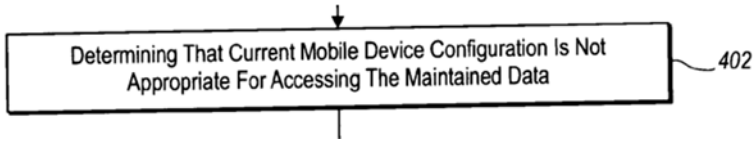
Limont discloses this limitation. EX-1003, ¶¶343-375. As noted for [1.1], the report received from the device indicates the current mobile device configuration in step 401. The configuration is used to determine if the existing policies need to be modified. For example, the server may "compare" the configuration in the request to other configuration versions ("*based on the report*") to determine that the request version does not permit the desired access of data on the server and therefore needs to be modified ("*determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified*").

> [0082] Method 400 includes an act of determining that current mobile device configuration is not appropriate for accessing the maintained

> data (act 402). For example, configuration enforcement module 193 can compare a configuration version included in request 176 to other configuration versions (e.g., included in configuration versions 192) that are appropriate for accessing data (e.g., Web pages in data store 197) maintained by server module 193B (e.g., a Web server). When the included configuration version does not match any other appropriate configuration version, configuration enforcement module 194 determines that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B. If no configuration version was included, policy enforcement module 193 can be default determine that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B.
>
> [0083] In response to detection of an inappropriate configuration, configuration enforcement module 143 can identify configuration settings, such as, for example, 191B, K, N, and R that are appropriate for accessing data maintained by server module 193B….

EX-1004, [0080-0083]; *see also* EX-1004, [0060-0065] for Fig. 2; [0045-0053] (describing various policy settings and versions). The act of "determining" that current settings are not appropriate (along with identifying the new settings that are appropriate as needed) corresponds to the claimed "*determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified*." EX-1003, ¶¶345-360.

Limont depicts this activity:



EX-1004 FIG. 4, step 402; FIG. 2, steps 202, 205.

The mobile device seeks to "access maintained data" on the server. EX-1004, [0079], [0089], [0060], Fig. 4 (step 405). That server data can only be accessed with the "appropriate" configuration settings (policies). Thus, determining that the current settings are "inappropriate for accessing data maintained by the server" (to which the mobile device seeks access) and identifying the correct settings is a determination that the mobile device's configuration settings (policies) "*need[] to be modified*" to allow the desired access. EX-1004, [0084-0089], [0060-0064]; EX-1003, ¶¶354-360, 374.

Limont's "configuration settings" includes policy settings, and Limont uses these terms interchangeably. EX-1004, [0073]. For example, Limont's "configuration enforcement module" 194 can be referred to as "policy enforcement module" 194 and "configuration settings" can correspond to "policy settings." EX-1004, [0077-0078], [0083]; *see also* "policy enforcement module 143" in EX-1004, [0045], [0055]. EX-1003, ¶¶362-369.

As detailed for [1.6], Limont's "configuration settings" (policy settings) can be sent from computer system 141 in steps 405, 206 for modifying the mobile device's configuration to permit the desired access to the server data (*a particular*

service policy setting … needs to be modified) of the mobile device (*the wireless end-user device*). EX-1004, [0085], [0089], [0065], Fig. 4; Fig. 2 . EX-1003, ¶¶370-374.

[1.3] the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting,

Limont in view of Wright and optionally Xu discloses this limitation. EX-1003, ¶¶377-441.

Limont's mobile device 101 includes a memory 112 that includes "program data 116" (**red**) (*partition*) that stores, for example, configuration settings 191B, K, N, and R and configuration version 192L (*the particular service policy setting being stored in … the wireless end-user device*). EX-1004, [0086], Annotated FIG 3.

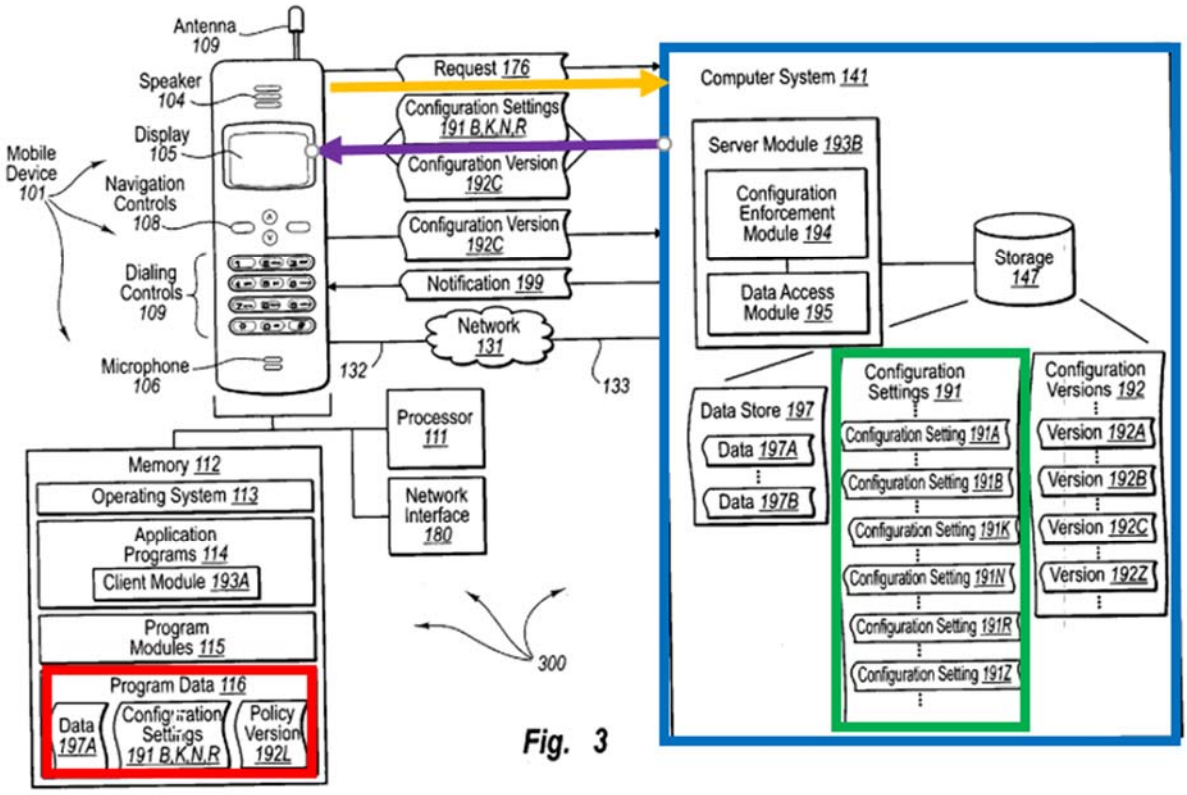


Fig. 3

EX-1004, FIG. 3. *See also* EX-1004, FIG. 1 (elements 191, 192, 171), [0044-0053] (storing policy settings and versions). EX-1003, ¶¶378-384.

Limont does not use the word that its partition is protected, but Limont does teach that the configuration settings of should be secure. A POSA understood that one well-known way to secure configuration settings was to encrypt or hide the configuration settings as taught by Wright (and optionally Xu) *to deter or prevent unauthorized modifications* to the mobile phone's settings. Section VI.A.4 EX-1003, ¶¶385-386.

For example, Wright identifies "security information" that may be encrypted that includes policies transmitted from the server to the mobile device.

> [R]esponsive to security information such as a policy or software being designated for encryption, the policy management module 236 provides 308 the designated client mobile device with cryptographic information which the client device can store and use to decrypt the security information. An example of cryptographic information is a key for use with a cryptographic authentication protocol. … permissions typically relate to the allowable modification that may be made to a downloaded policy or client software by the client mobile device.…

EX-1005, [0078]. Wright also describes various "permissions" for the policies which also protect the policies as recited in this element because they specify the ability to modify (or not modify) the policies. EX-1005, [0078-0103], [0280-284]; EX-1003 ¶¶387-389.

"Examples of security information are versions of existing policies, policies, or software." EX-1005, [0051]. *See also* EX-1005, [0061]. Wright thus discloses "protected partitions" through: (1) storing encrypted security information (policies); (2) the ability to "hide" the policy file and (3) "permissions" for policies. EX-1005, [0014], [0103], [0262], [0280-0284]; EX-1003, ¶¶387-394.

Wright details "aspects of" policies such as rules, permissions, network environments, locations, security features, network services, ports, applications and the actions (enforcement mechanisms) which generally correspond to Limont's policy disclosures. EX-1005, [0048], [0180-0184] Figs. 5B-5F; EX-1003 ¶¶395-398.

Wright shows a specific "*protected partition*" in "memory 220":

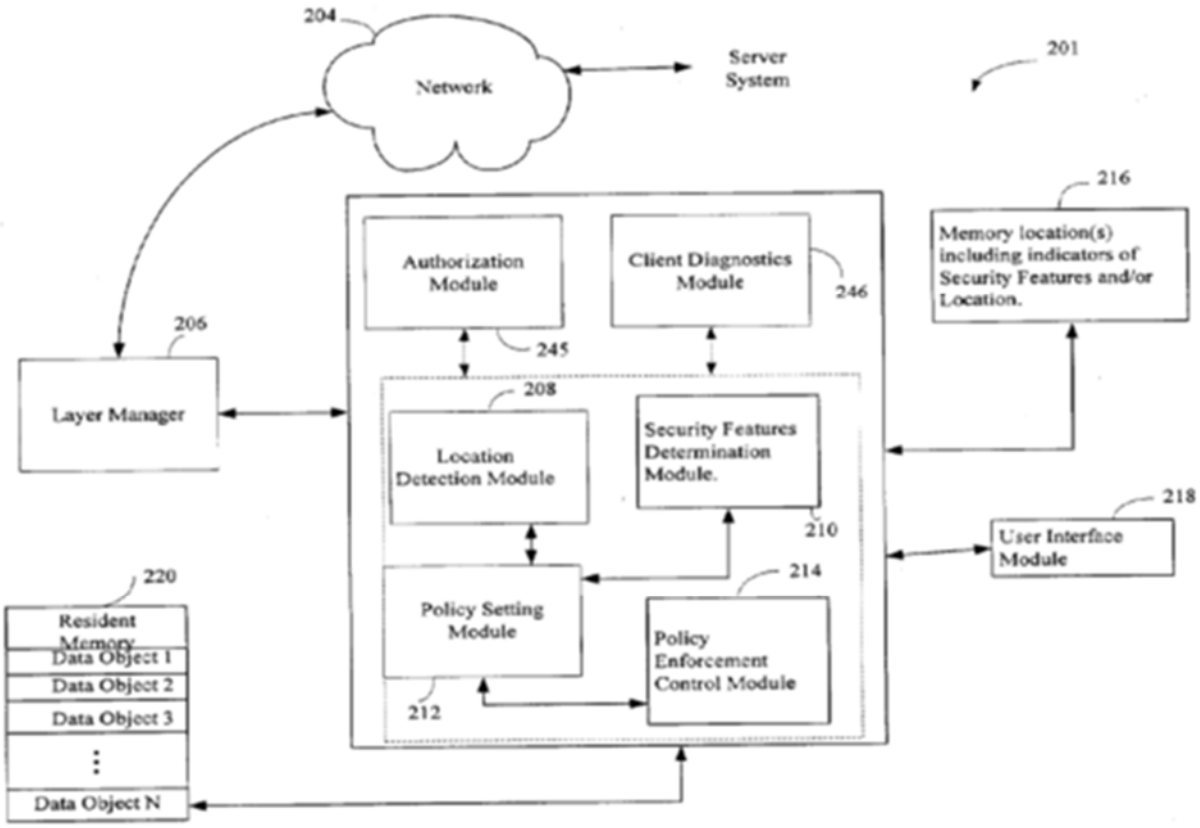


FIG. 2B

EX-1005, Fig. 2B. Memory 220 stores policies and is protected by encryption (and hiding) and policy evaluation from elements 208, 210, 212, and 214. EX-1005, [0047], [0058-0060], [0176-0177], [0280]; EX-1003, ¶¶395-409. In the proposed combination, for at least the stored policies, Limont's memory 112 would be implemented as is described for Wright's memory 220 (including, as necessary, Wright's modules that provide the encryption/decryption capabilities and controls). EX-1003, ¶410.

Wright addresses the same issue identified by Limont in that the mobile device's "location" may impact the need for a "security policy" that protects the data (by encryption or hiding as per a policy) differentially – for example on whether a location is secure or not. EX-1005, [0014]. EX-1003, ¶¶410-412.

Thus, Wright provides a solution for the problems identified in Limont of: (1) unauthorized access to secure data (such as policies) on a mobile device; (2) allowing an administrator to lock down the policies on the mobile device; and (3) allowing an administrator to remotely administer/update policies wirelessly. EX-1003, ¶413. Wright's solution provided for the encryption of the device's secure data (and the ability for the administrator to authorize access to the encrypted data). EX-1005, Figs. 2B, 3C; [0131-0132].

Wright's disclosure of using encryption to provide a "*protected partition of the wireless end-user device*" is consistent with the '042 Patent disclosure where "the memory protection function includes encrypting traffic to and from memory so that only authorized device program elements possess the counterpart encryption capability to access the memory." EX-1001, 9:27-30. EX-1003, ¶414.

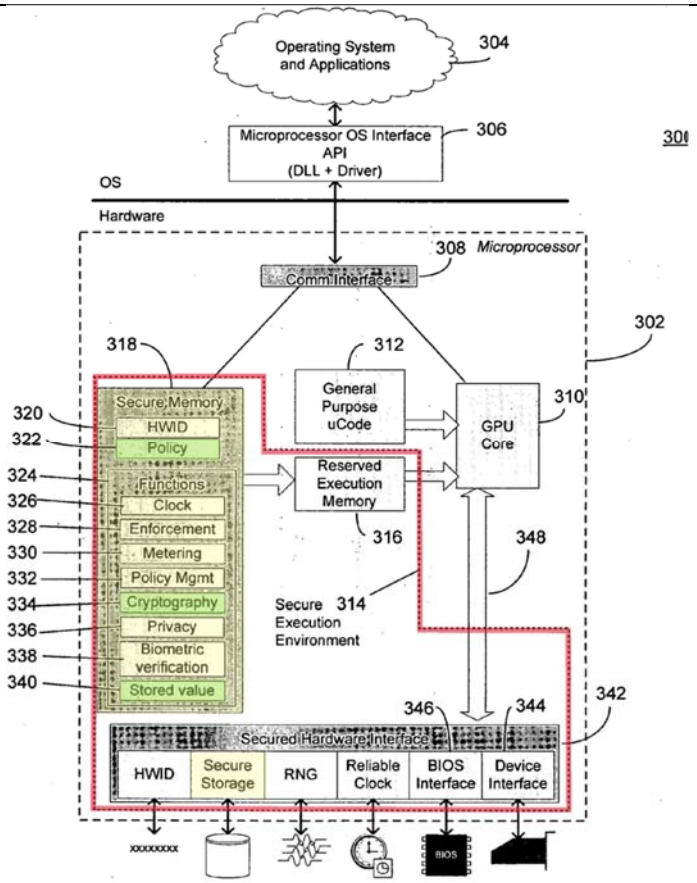
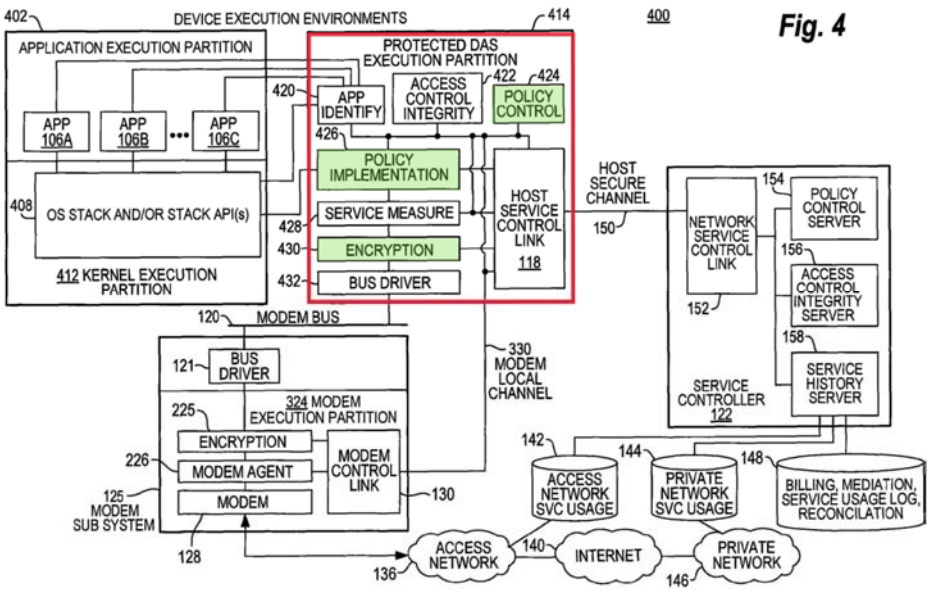
Thus, Wright's disclosure of memory storing encrypted policies teaches the claimed "*the particular service policy setting being stored in a protected partition of the wireless end-user device*." If PO argues that the "protected partition" requires functionality beyond "storing" data, then Wright's "protected partition"

would include the components and modules in Fig. 2B (along with the processor and buses) used to control encryption / decryption. EX-1005, Figs. 2B, 3C; [0131], [0047], [0051], [0062]; EX-1003, ¶415.

Wright's "*protected partition"* is *"configured to deter or prevent unauthorized modifications to the particular service policy setting*" because the encryption (and hiding/permissions) prevents unauthorized users from modifying the policies stored in Wright's encrypted memory. EX-1005, [0078-0104], [0229-0230], [0259-0264], [0280-0284], [0048]. EX-1003, ¶416.

A POSA would have understood that Limont's data (e.g., policy settings) should be protected to further limit access which "reduce[s] the likelihood of a compromised device or a device with noncompliant policy setting being able to access data" as taught by Wright and would be confident of its success. EX-1004, [0071]. EX-1003, ¶417. *Supra* Section VI.A.3.

To the extent that PO argues that the "*stored in a protected partition*" term requires that the partition be "secure execution environment" as depicted in the embodiment shown in '042 Patent's Fig. 4 or specific hardware controls, then Xu supplies such a secure execution environment. EX-1003, ¶¶418-440. As shown below, the '042 patent largely copies the secure execution environment functionalities disclosed by Xu of policy control/management and encryption. EX-1003, ¶419.

Xu Fig. 3	
'042 Fig. 4	

Xu "provides a secure base for enforcing security and/or operating policies, …for use in … an electronic device such as a computer, cellular telephone, personal digital assistant… The processing unit may include … secure storage [and] … a cryptographic unit… to establish the basis for computer capable of being operated in compliance to a usage policy." EX-1016, [0003]. Xu's "secure execution environment" includes "secure memory … in a tamper resistant manner [to store] … policy data 322 that may specify policy related operational directives such as metering, reporting, update requirements, etc. … [and] implement various functions … includ[ing] … policy management, cryptography…." EX-1016, [0023]. EX-1003, ¶¶420-422.

Xu's "secure memory" stores policies "in a tamper resistant manner" and thus, is "***configured to deter or prevent unauthorized modifications***" to the stored policies. EX-1003, ¶¶423-426; EX-1016, [0032].

The proposed combination modifies Limont's teaching of memory 112 to implement a secure memory for at least the portions storing Limont's configuration/policy settings and versions as taught by (which corresponds to Xu's "policy data 322") as taught by Xu. Any other aspect of Limont's memory 112 needed for the policies would likewise be included in secure memory. EX-1003, ¶427-432.

Xu's secure environment also provides functionality to execute Wright's encryption protections using cryptography function 334 and store related encryption keys. Xu's "cryptography function 334 may be used for digital signature verification, digital signing, random number generation, and encryption/decryption." EX-1016, [0025]. The "policy" management includes numerous different policies. EX-1016, [0029-0032]. EX-1003, ¶¶428-431. Indeed, Xu teaches that the cryptographic function is used for policy updates. EX-1016, [0025], claim 9.

A POSA would be motivated to implement a secure environment as taught by Xu on Limont's mobile device incorporating Wright's encryption functionality. EX-1003, ¶¶431-440. A POSA would recognize that all three references were assigned to leaders in the data policy management field (Microsoft and Apple). All three references provide complementary solutions for updating and protecting sensitive data, including specifically policies, for mobile devices. Moreover, a POSA would have been motivated for such a combination because it was well-known long before the '042 Patent to provide for the protection of data in mobile devices using techniques such as hardware protections and encryptions. See Section IV.F.3 (detailing known techniques). EX-1003, ¶¶263-267.

Using a secure environment as taught by Xu addresses Limont's concern regarding "malicious users" accessing confidential information if "a mobile phone

[is] lost or stolen" by controlling the device at boot-up. EX-1004, [0013]; EX-1016, [0030]. Xu's secure environment also beneficially stores the encryption keys for confidential communication, including policy updates. EX-1003, ¶¶279-286, 435-436.

A POSA would also have been further motivated to modify Wright's encryption functionality using a secure environment as taught by Xu. For example, Wright's usage of "cryptographic information which the client device can store and use to decrypt the security information" to protect "keys" and "cryptographic authentication protocols" for protecting files, software and policies benefits from a secure environment which protects such cryptographic algorithms and keys from unauthorized access. EX-1005, [0078], EX-1016, [0025-0026]. As detailed above, Wright teaches encrypting policy updates and Xu beneficially augments that teaching by allowing for cryptographic verification of such updates and to "establish trust" to outside entities (such as Limont and Wright's servers) to perform such updates "between client and server … through a secure channel." EX-1016, [0025], EX-1005, [0267]. Thus, the teachings of Xu beneficially increase Limont's and Wright's protections for traveling users at risk of having their devices lost and stolen and which devices may need to be updated with new policies in unsecure environments using wireless channels. EX-1003, ¶437.

A POSA would have a reasonable expectation of success in the combination. Utilizing a secure environment provides the functionality to implement storage and encryption as described in Limont and Wright. The combination is merely well-known functionality operating in it known and predictable manner to achieve a known and predictable result (the storage of data and the execution of instructions on a microprocessor). EX-1003, ¶438. Notably, the '042 Patent does not describe any improvement to known techniques for such "protected partitions" but rather relies upon the knowledge of a POSA. EX-1003, ¶¶439-440. Such knowledge is correspondingly available to a POSA in assessing obviousness.

[1.4] the particular service policy setting being associated with a service profile[2] that provides for access by the wireless end-user device to a network data service over a wireless access network,

Limont discloses this limitation. EX-1003, ¶¶443-470. Limont's "[m]obile device 101 can wirelessly exchange data" and "include[s] network interface 180 that can, when appropriate, interoperate with antenna 109 to receive data from external sources and/or transmit data to data." EX-1004, [0041]. Limont also discloses a configuration version (*service profile*) as a set of data including one or more configuration settings (*service policy setting*). EX-1004, [0075], [0045-0053]

[2] The '042 Patent specification does not recite the term "service profile" or even "profile."

(describing various policy settings and versions). Limont also discloses the configuration settings of the mobile device (*wireless end-user device*) can include "a **network interface**, and **wireless protocol settings**." EX-1004, [0087]. Limont's communication links may use wireless protocols (e.g., GPRS, GSM, etc.) *over a wireless access network*. EX-1004, [0043], [0056]. EX-1003, ¶¶444-446.

Thus, a POSA understood that this "access" along with the network interface and wireless protocol settings are *service policy settings that provides for access … to a network data service over a wireless access network* because the network interface controls the transmission/reception of data from the mobile device, and the wireless protocol specifies the format of the data wireless transmitted over the wireless access network to the mobile device. EX-1003, ¶¶447-451.

Limont describes several forms of specific services with distinct accessed data also corresponding to the "*network data service*." For example, Limont's server module 193B on a computer system could be an electronic mail server, or a web server that communicates with the mobile device using protocols including TCP/IP and other higher layer protocols, Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP), etc. over network 131 (*access by the wireless end-user device to a network data service)*. EX-1004, [0038], [0045], [0073].

Moreover, as discussed in [1.2] and [1.3], Limont's policies are intended to allow "*for access by the wireless end-user device to a network data service*" providing the data on/from the server. EX-1003, ¶¶452-466.

Limont's server module 193B interoperates with client programs (*e.g.,* client module 193A) to transfer data (*e.g.,* Web pages) to mobile device 101. Policy enforcement module 194 determines if a requesting mobile device's policy settings are appropriate for accessing data specific to a service. EX-1004, [0077]. Thus, a POSA understood that server module 193 (or 142) provides *access to a network data service over a wireless access network*. EX-1003, ¶¶467-469.

[1.5] the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and

Limont discloses this limitation. EX-1003, ¶¶472-477.

As discussed in [1.2], [1.3] and [1.4] above, Limont's server 142/193 evaluates the configuration / policy settings (*particular service policy setting*) to determine if those policies allow for access to specific data requested from the service. The policy settings are modified (if needed) to be appropriate to access the requested server data (*one or more communications associated with the wireless end-user device over the wireless access network*").

Whether the device's settings are "appropriate to access the data" determines ("*control[s]*") whether the server communicates the requested data back to the

mobile device and therefore "*the particular service policy setting"* is *"configured to assist in controlling one or more communications*." EX-1003, ¶¶473-474. Furthermore, as detailed in element 1.4, Limont's policy settings can be specific to different types of communications such as e-mail and HTTP web service. EX-1003, ¶¶452-466, 475.

Additionally, Limont discloses that implemented configuration settings can alter the current configuration for a network interface, and wireless protocol settings, at the mobile device which is a separate form of "*control one or more communications associated with the wireless end-user device over the wireless access network*." EX-1004, [0073], [0087], EX-1003, ¶476.

[1.6] in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.

Limont discloses this limitation as detailed in [1.2], [1.3], and [1.4]. EX-1003, ¶¶479-486. Element 1.1 discusses Limont's the *service control link.* Limont discloses *determining that the particular service policy setting needs to be modified* as discussed in [1.2], [1.3] above.

Limont sends modified device configuration (policy) settings to the mobile device (purple) (*sending configuration information to the wireless end-user device*). EX-1004, Fig. 3; Fig. 1 (transmission of "settings 117" and "Policy Version 118D"); [0065]. After being sent the modified configuration settings,

"[m]obile device 101 can implement settings 117A, B, F, and H (potentially altering current policy settings) ["*configured to assist in modify or allowing modification to the particular service policy setting*"] to comply with policy settings that are appropriate for accessing data maintained by server module 142B." EX-1004, [0066]. *See also* EX-1004, [0065], [0086-0087], claim 6. The device configuration setting represents a modified mobile device configuration that is appropriate to access the maintained data on the server. EX-1004, [0084-0089], Fig. 4 [step 403]. EX-1003, ¶¶480-484.

The *configuration information* for the configuration/policy settings to access the network data service (*e.g.*, email) on the server and for the network interface and the wireless protocol setting is discussed in claim element 1.4 above. EX-1003, ¶¶484-485.

b. <u>Claim 2</u>

[2.0] The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control.

Limont discloses this limitation. EX-1003, ¶¶488-494. Element 1.2 discusses Limont *particular service policy setting*. Limont's configuration settings 191B, K, N, and R (*the particular service policy setting*) can correspond to any of the previously described policy settings as well as "[t]he current configuration of one or more of an operating system an application program, hardware, allocated

resources, a network interface, and wireless protocol settings, at the mobile device." EX-1004, [0083], [0085].

A POSA understood that configuration settings related a network interface or wireless protocol can *assist in implementing roaming control*. For example, the ability to control (via policies) the wireless protocol settings allows for control of roaming by preventing (or allowing) access to specific wireless protocols and networks. EX-1003, ¶¶490-491.

Moreover, Limont specifically identifies (as a problem solved by Limont) the inability of system "administrators" to control the configuration of mobile devices – particularly to protect sensitive information that may be "private." EX-1004, [0006-0015]. Furthermore, given that Limont includes the ability for an authority figure (e.g., "administrator") to oversee individual with less access privilege (e.g., users), a POSA understood that Limont's system would assist in implementing a "parental control" in which an analogous authority figure (parent) oversee individuals with less access privileges (children). EX-1003, ¶492. The specific terminology of "parental" does not impact the underlying control by the authority figure.

Limont's mobile device connects to networks such as "a Local Area Network ('LAN'), a **Wide Area Network ('WAN')**, or the Internet" using "wireless protocols (e.g., GPRS, GSM, etc….)." EX-1004, [0034], [0038], [0043],

[0056]. Those networks include "an **office-wide** or **enterprise-wide computer network**, an intranet, and/or the Internet." EX-1001, [0041]. Therefore, Limont's managed network expressly includes an "enterprise-wide" wide-area networks, which a POSA understood was a WWAN.

Thus, a POSA understood that a mobile device having configuration settings that can be used to modify the hardware, network interface, allocated resources, and wireless protocol settings to connect wirelessly through the internet or other wide area network can be used to *assist in implementing enterprise wireless wide-area network (WWAN) management control* for the corporate wireless mobile devices managed by the "administrator." EX-1003, ¶¶493-494.

f. Claim 6

[6.0] The method of claim 1, further comprising: obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and

The proposed combination discloses this limitation. EX-1003, ¶¶496-506. Limont's settings can be based on "if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time" and the mobile will "verify download speed" (*obtaining a service usage measure*). EX-1004, [0073], [0086]. These measurements *account[] for the one or more communications*

associated with the wireless end-user device over the wireless access network). EX-1004, [0077]. EX-1003, ¶¶497-498.

Additionally, Wright's client diagnostic modules (detailed in claim 11) provide "usage" logs to the server which correspond to this claim element. EX-1005, [0220], [0225] ("network service usage" information]; [0270] (referencing service usage measurements such as "program usage, network access… VPN access, data access…]). EX-1003, ¶499.

[6.1] based on the service usage measure, taking an action.

Limont's mobile devices verify the speed (*service usage measure*). Limont's system takes four separate *actions based on the service measure* and whether the measure is appropriate for the requested data: (1) if the measure is inappropriate, then the server prevents the data transfer and then modifies the settings (both *actions*); and (2) if appropriate, the server allows/makes the transfer and notifies the mobile (both *actions*). EX-1004, Fig. 4, [0086], [0091], [0077-0078]. EX-1003, ¶¶500-501.

Additionally, Wright's diagnostic modules perform diagnostic *actions based on* the usage logs as detailed in claim 11, *infra*. EX-1005, [0046], [0052-0054], [0057-0059], [0068-0077], [0220]; EX-1003, ¶502.

Limont's disclosure is consistent with the '042 Patent's disclosure identifying a "service usage measure[]" as "projected traffic demand [and]

application usage … reported to the servers for the purpose of provisioning the right amount of data bandwidth … to the device." EX-1001, 13:59-14:2; EX-1003 ¶503.

g. Claim 7

[7.0] The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity.

Limont and Wright each disclose this limitation for the reasons discussed for Claim 6 where the *service usage activity* is downloading data (Limont) or "network usage" (Wright). EX-1004, [0086]. EX-1003, ¶¶505-506.

h. Claim 8

[8.0] The method of claim 6, wherein the action is to verify the service usage measure.

The proposed combination discloses this limitation. EX-1003, ¶¶508-515. As discussed for Claim 6, Limont's "action" can be Limont preventing the transfer of data or transfer the appropriate configuration settings to the mobile, if the configuration setting are inappropriate. EX-1004, [0078], [0091]. Limont further discloses that one action resulting from the measurement (or comply with modified settings) is to verify the download speed (*verify the service usage measure*). EX-1004, [0086]. EX-1003, ¶508.

Additionally, Wright's "remote diagnostics module 224 [discussed below for claim 11] may also probe a particular client to verify its status" including "policy

settings on the device, and attributes in accordance with those settings, for example, which ports are blocked." EX-1005, [0057]. Wright's diagnostic module also orders "audits" and receives "audit logs" (including the results of "tests") which a POSA would understand to render obvious the verification of service usage in light of Wright's policies specifying network usage and data access. EX-1005, [0054], [0068], [0076-0077], [0104-0123], [0138], [0269] EX-1003, ¶¶509-513.

Wright also describes such verification of applications, protocols, and VPN service usage as well as files, checksums, and registry entries for which it would have been obvious to base such actions on Wright's service usage logs to perform additional actions such as the repair describe in claim 11 below. EX-1003, ¶¶514-515.

i. Claim 9

[9.0] The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device.

Limont discloses this limitation. Limont discloses preventing the download of data (*action is to suspend*) to an inappropriately configured mobile device (*wireless end-user device*) as detailed in [1.2], [1.3], [1.4] which provides benefits. EX-1004, [0091]. EX-1003, ¶¶517-520.

Limont also discloses a "wipe" action which a POSA would recognize as quarantining or suspending the device because the "wiping" would remove the information needed to access data. EX-1004, [0047-0049], [0071]. EX-1003, ¶520.

j. Claim 10

[10.0] The method of claim 6, further comprising obtaining secondary information associated with the wireless end-user device, and wherein the action is to verify the service usage measure using the secondary information.

The proposed combination discloses this limitation. EX-1003, ¶¶522-525. As discussed for Claim 6, Limont discloses obtaining a service usage measure in the form of download connection speed. Further, Limont discloses obtaining information regarding the correct plug-ins on a mobile device, and information regarding whether sufficient resources have been allocated to a mobile device (*obtaining secondary information associated with the wireless end-user device)*, in order to determine if sufficient resources have allocated at a mobile device or if a mobile device includes correct plug-ins for viewing content (*action is verify the service usage measure using secondary information*). EX-1004, [0077], [0086]. EX-1003, ¶¶523-524.

As detailed for claims 6, 8, and 11, Wright's diagnostic module requests, and receives diagnostic information (including network usage information) from

the mobile client ("secondary information") and performs processing on those logs. A POSA would understand this to render obvious the claimed verification for the reasons stated in claim 8. EX-1003, ¶525.

k. Claim 11

[11.0] The method of claim 1, further comprising receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation.

Limont in combination with Wright discloses this limitation. EX-1003, ¶¶527-538. As discussed in the Motivation to Combine section above, Limont discloses that the policy settings should be "locked down" and protected on the wireless device, but does not expressly disclose an integrity report to assist a network element in identifying an access control integrity violation.

Moreover, Limont discloses the ability to remotely "wipe" data on the mobile device (including wipe's controlled by Limont's server [*network element*]) to "limit the ability of malicious user to access data." EX-1004, [0047-0049], [0071]. A POSA would have recognized the value of receiving integrity information that would allow the server to determine if the mobile's data needs to be "wiped." EX-1003, ¶¶528-529.

However, Wright discloses a client diagnostics module 246 on the wireless mobile that performs audits of all files to verify no corruption (e.g. checksum) (*integrity report*) and for security violations. EX-1005, [0068-0073]. EX-1003,

¶¶530-533. The '042 Patent identifies "checksums" as an integrity check. EX-1001, 17:6-23.

A remote diagnostics module 224 (*network element*) and analyzes the audit information received from the mobile device to independently determine "problems … with security." EX-1005, [0053]. The information transmitted to the server includes "current version of the security policy software components on the client device" which would also allow the server to potentially determine if the secure information has been altered or corrupted. EX-1005, [0057]; EX-1003, ¶¶534-535.

The remote diagnostic module may repair client device problems, determine that a trend is occurring for the device, or schedule preventive maintenance (*receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation)*. EX-1005, [0046], [0052-0054], [0057-0059], [0068-0077], [0220]; Fig. 11. In Wright's system "support information may be in the form of instructions or code to the client device to repair a problem or perform maintenance" which "provides an advantage of taking corrective or preventive actions without requiring user intervention or action." EX-1005, [0055]. Wright's client "may also run tests with respect to the security policies" such as security violations with the output of such tests transmitted to the server. EX-1005, [0076]. EX-1003, ¶536.

A POSA would have been motivated to modify the Limont's teachings to include a diagnostic module to audit the policy settings as taught by Wright in order to protect and lockdown the policy settings on the wireless device. Such integrity reports provide information to Limont's administrator that secure data (such as encryption keys, user-id, passwords, and PINs) have been compromised thus allowing the administrator to take corrective action such as the "remote wipe" discussed above. EX-1004, [0047-0049]. EX-1003, ¶437.

Wright's audit (integrity report) matches the '042 Patent disclosure audit scans of memory and files on the wireless device to detect unauthorized data using checksums or other information. EX-1001, 10:3-20. EX-1003, ¶538.

k. Claim 12

[12.0] The method of claim 1, wherein the configuration information comprises at least a portion of the service profile.

As noted in [1.6], the claimed "*configuration information*" is sent from the server to the mobile device to modify at least one of the "*service policy settings*." As discussed for element [1.4], Limont's "*service profile*" is a "group of one or more configuration settings" identified by Limont's "configuration [policy] version." EX-1004, [0075]. For example, Limont identifies an exemplary "group of one or more configuration settings" ("service profile") using a configuration / policy "version." EX-1004, [0073], [0075]; Fig. 3. EX-1003, ¶¶540-546.

Limont's Fig. 3 shows Limont's "configuration settings" (e.g., settings 191B, K, N, R) transmitted to the mobile device in the **purple arrow**.

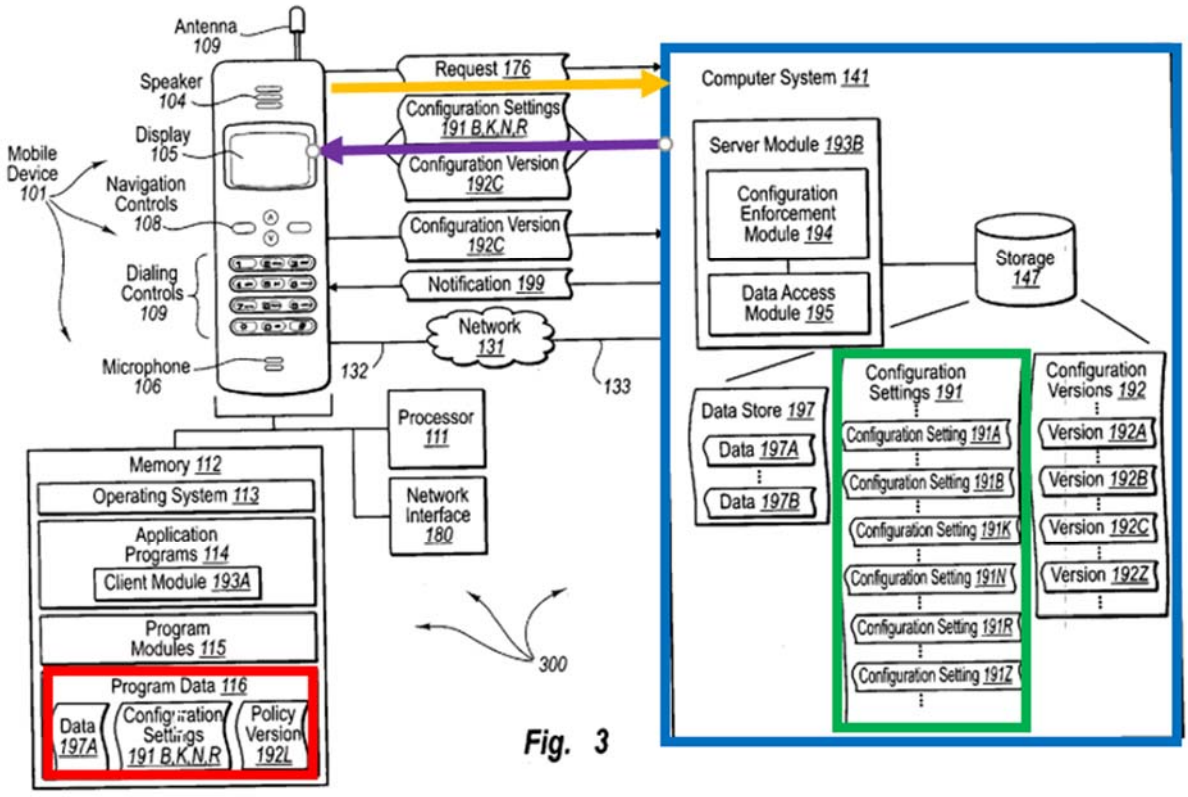


Fig. 3

EX-1004, Fig. 3.

Each transmitted "configuration setting" is "*a portion*" out *"of the service profile*" (the group of these four settings identified by the "version") as is the "version 192C." EX-1003, ¶¶545-546. This analysis applies for the Fig. 1 components (settings 117, version 118D). EX-1003, ¶¶543-546.

l. Claim 13

[13.0] The method of claim 1, wherein the service control link is secured by an encryption protocol.

Element 1.1 discusses communication links 132, 133 (*service control link*). Limont further discloses computer systems receiving a policy update to use "a specified version of encryption algorithm." EX-1004, [0009]. Furthermore, Limont teaches that "wireless protocols" such as "GPRS [and] GSM" are used for the communications link. A POSA would understand that such wireless protocols use encryption protocols to protect the data transmitted wirelessly (or else every device could intercept such data) or, at a minimum, that it would be obvious to use such encryption protocols for wireless transmissions. EX-1003, ¶¶549-553, 154-157 (citing EX-1006).

Moreover, Wright further discloses types of network services according to a policy can include service protocols for transferring data over a network (*service control link*). The service protocols can include Virtual Private Network (VPN) and HTTPS which encrypt the data across the communication link. EX-1005, [0009], [0223], [0279], FIG. 8 (element 820). EX-1003, ¶¶554.

In addition, Wright discloses TLS and SSL service protocols which are known to encrypt data/communications over the network including for VPNs. EX-1005, [0265-0267], [0279]. A POSA would be motivated to modify Limont's teaching that: (1) wireless devices are less secure (and therefore would benefit by securing the links with encryption) and (2) by encrypting the communication links

to allow secure communication between the wireless device and computer as taught by Wright for the reasons discussed in the Motivation to Combine section. Xu identifies the using encryption to "establish trust" for policy updates and thus provides additional motivation to combine encryption into Limont's communication links. EX-1016, [0025]. EX-1003, ¶¶555-557.

m. Claim 14

[14.0] The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.

Limont discloses several examples of this limitation as also detailed in element 1.1. EX-1003, ¶¶559-565. For example, Limont configuration version (*service profile setting*) is a reduced set of data that represents one or more configuration settings. EX-1004, [0075]. Limont's mobile device's policy settings include the mobile device connection speed (*service usage policy setting*) sufficient to download a Web page in a reasonable period of time. EX-1004, [0077]. EX-1003, ¶¶561-565. As detailed in element 1.1, these different settings are transmitted from the device to the network as part of the device service state.

n. Claim 15

[15.0] The method of claim 1, wherein the device service state provides information about a user preference.

Limont discloses that policy settings reflecting the device service state can include Personal Identification Number ("PIN") lock activation settings, which

provide information about a user preference because the user's selection of a "PIN" discloses, or renders obvious, a user preference. EX-1004, [0047-0049]. EX-1003, ¶¶568-570.

Moreover, Limont's request 176, request 164, and command 161 (*information about device service state* as per element 1.1) indicate the user's selection (preference) as to the specific data (including types such email, web content or other data) the user wants to access. EX-1004, [0044], [0054-0055]; [0067-0069], [0080]. EX-1003, ¶¶571-572.

Wright's teachings include that there is a "settings application" on the mobile device giving a user the "[a]bility to modify" or "override" settings such as "visual settings" and "location." EX-1005, [0078-0103]. Wright's "user interface module 218" allows users specify "supplemental policy definitions or customization of policy definitions based upon user input" and other "aspect of a policy." EX-1005, [0061], [0065], [0173], [0178]. Such "settings" and user-customizable policy aspects are part of the *device service state* and are *information about a user preference* or render those elements obvious. EX-1003, ¶572.

Furthermore, a POSA would understand that it would be obvious that a mobile device would store "*information about a user preference*" as part of its state of its device to provide services to a user. EX-1003, ¶573.

o. Claim 16

[16.0] The method of claim 1, wherein the device service state comprises information associated with an encryption key.

Limont's "[p]olicy updates" may force using a "specified version of encryption algorithm [and] a specified key length." EX-1004, [0009]. This information is "*information associated with an encryption key*" that is part of the device's service state. EX-1003, ¶¶577-578.

.

Although, the claimed "information" is not required to be transmitted,, Limont in view of Wright discloses this limitation. As detailed in element 1.3, Wright's mobile device uses "cryptographic information" which is a "key for user with a cryptographic authentication protocol" that is stored in configuration information such as policies sent to the mobile device. EX-1005, [0078-0103]. Thus, when Limont transmits its stored "policy settings" (*see* element 1.1), those settings would include the encryption keys (or, at a minimum, information associated with an encryption key) associated with the policies. EX-1003, ¶579-580.

Wright's keys allow the mobile device to authenticate updated policies. EX-1005, [0130-0131]. Moreover, Wright's communication between the mobile device and the server (to send / receive, for example, Limont's policy settings) uses a secure protocol that involves the transmissions of "information associated with

an encryption key" to establish the session. EX-1005, [0133-0159]. EX-1003, ¶581.

A POSA understood that using an encryption key to limit access to stored data "reduce[s] the likelihood of a compromised device or a device with noncompliant policy setting being able to access data" and would be confident of its success, as discussed in the Motivation to Combine section. EX-1004, [0071]. EX-1003, ¶582.

p. Claim 17

[17.0] The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.

Limont and Wright discloses the *device service state* as discussed with reference to claim element 1.1 and further discloses a *service usage* measure (*record*) as discussed in Claim 6, and further discloses an *integrity report* as discussed in claim 11. Wright discloses a *transaction record* in its "status, configuration, error logs, audit logs, and debug information" and "event logs." EX-1005, [0269], [0079], [0197]; EX-1003, ¶¶584-591.

Although not claimed, a POSA understood that these portions of the device service could be transmitted to the server to "determin[e] if a requesting mobile device's policy setting are appropriate for accessing data." EX-1004, [0077]; EX-1003, ¶591.

q. Claim 18

[18.0] The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.

As discussed for claim limitation 1.1, Limont teaches that the configuration settings (*device service state*) can include application program settings (*application status information*). Furthermore, Limont's server module determines whether sufficient resources (*device status information*) have been allocated at the mobile device in response to the mobile device request, which can include determining if correct plug-ins for viewing content are included at the mobile device (*application status information*) or if the mobile device connection speed to download a webpage can be accomplished in a reasonable amount of time (*device QOS/device status information*). EX-1004, [0077]. Wright's *device service state* stores and uses the *device location*. EX-1005, FIGs. 2B, 3A; 3D-3E , [0174-0212]. EX-1003, ¶¶593-598.

B. Ground 2: Claims 3-5 are obvious over Limont in view of Wright and Xu and in further view of Polson.

Ground 2 addresses Challenged Claims 3-5 that recite an "intermediate networking device" that "forwards" data or "assists" other devices in communicating. Polson describes the type of client device used in Limont's network. Polson's client device acts as a gateway between the WWAN and WLAN to forward data between the two networks pursuant to policies programmed by the network. EX-1003, ¶¶600-695.

1. Polson

Polson teaches a "gateway" between WWAN and LANs (wireless and wireless). Polson broadly defines "gateway:"

> "[G]ateway" refers to any computing device capable of facilitating transmission of data from one or more LANS to one or more WWANs, and transmission of data from the one or more WWANs to the one or more LANS.

EX-1008, [0026]. For example, Polson's gateway establishes a forwarding link between a WWAN network (*e.g.*, a cellular network) and a WLAN network (*e.g.*, an 802.11 network). EX-1008, [0022-0023], [0051-0056]. Polson's "routing engine" forwards between networks. EX-1008, [0020].

Polson describes "portable" gateway embodiments carried by a user permitting "teams of users" to use the WWAN / cellular connection by connecting

to the WLAN. EX-1008, [0027]. Polson's gateway creates a wireless "hotspot" allowing WiFi devices to share a cellular connection. EX-1003, ¶¶120-130.

Polson's gateway includes extensive ability to download and enforce policies from the cellular network controlling use of the WWAN and WLAN connections. As detailed for claim 5, Polson identifies numerous policy types implemented by the gateway – including "customized" policies specific to a "large corporate user." EX-1008, [0037]. These policies are enforced by "subscriber determination logic." EX-1008, [0020], [0029-0042], [0056-0058], claim 24.

Polson's gateway downloads new policies wirelessly from the wireless service provider including policies that restrict or allow the LAN users to access the WWAN network. EX-1008, [0032-0034], [0078]. These gateway / server interactions allows user to change their service plan resulting in policy updates. EX-1008, [0031], [0078]; claims 7, 19.

2. Motivation To Combine Polson With Limont, Wright and Xu.

Polson provides a client device that fits Limont like a glove. EX-1003, ¶¶604-639. Limont teaches managing, enforcing, and updating configuration settings (policies) on client devices such as mobile devices. EX-1004, Title, [0016-0018].

> A "mobile device' is defined as a subset of computer systems that primarily (or solely) access networked data using wireless mechanisms and are easily transportable by a human….

EX-1004, [0036]. However, Limont's "invention" encompasses "personal computers, laptop computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs…." EX-1004, [0037].

Polson's "gateways" are "any computing device" capable of forwarding data between WWAN and WLAN networks. EX-1008, [0026]. Polson's gateway embodiments are "easily transportable by a human."

> [0027] [G]ateway 108 may be adapted to be powered through … an internal or external battery. Inclusion of the [battery] power supplies enables the gateway 108 to be used in portable settings. For example, teams of users may carry the gateway 108 in a briefcase or bag.

EX-1008, [0027]. Thus, Polson's gateway meets the category of Limont's devices benefiting from Limont's policy management system. EX-1003, ¶¶605-615.

Limont' problems to be solved include allowing corporate administrators to ensure that policies can be updated for devices used by employees outside the normal "wired" offices. EX-1004, [0005-0015]. EX-1004, [0010]. Thus, corporate administrators needed solutions (as provided by Wright, Xu, and Polson) for enforcing policies for traveling users.

A POSA would have recognized that Polson's teaching of a mobile/portable gateway supplements Limont's teaching of policy management for traveling users. EX-1003, ¶¶616-620. A POSA would have recognized that Polson's added layer of policy enforcement at the WWAN/WLAN gateway can be used to supplement (or even replace) the policy enforcement of other end-user devices (such as mobile phones or laptops), particularly for travelers. EX-1003, ¶621.

Polson provides a similar solution to Limont, Wright and Xu. Polson's gateway allows for downloading customized policies specific to subscriber agreements and such "customization may be implemented by a wireless service provider for a certain customer, for example for a large corporate customer of the wireless service provider." EX-1008, [0037]. Thus, Polson's teachings would add the benefit to Limont of applying customized corporate policies across all corporate users of the WLAN provided by Polson's gateway. EX-1003, ¶¶62.

Furthermore, as noted in element 1.1, Limont's policies on the mobile devices may be modified to reflect additional needs of mobile users such as changing the speed or wireless networks/protocols. Polson matches this ability in allowing for its mobile users to change their subscription as needed and update the related policies to match the new capabilities of the subscription.

> [T]he subscriber determination logic of gateway 108 may facilitate a subscriber in altering their existing WWAN 112 access ability … the subscriber may be able to change their service agreement to one that

> allows for WWAN 112 access via gateway 108, or to purchase WWAN 112 access on another basis, e.g., a certain period of time, a certain quantity of bytes downloaded, etc. An example of a service agreement that does not permit use of gateway 108 may be a service agreement that envisions the subscriber only being able to use a single computer at a time to access the carrier's WWAN 112. Another example of a service agreement that doesn't permit a gateway 108 is one that's designed specifically for a phone. In a subset of such an example, the service agreement may permit use of gateway 108, but only in connection with a single computer at a time.

EX-1004, [0031]. Limont's management system provides the vehicle for altering Polson's WWAN/WLAN access policies. EX-1003, ¶623.

Polson's "gateway may also facilitate a subscriber in altering the features of his/her service agreement" and change features such as "a quality of service, a throughput limitation, and a data transfer rate limitation" that are provided in "policies" transmitted to the gateway by a "server." EX-1008, [0078-0079], Fig. 8. Limont similarly describes that a "server" sends the policy updates to the clients to modify the service (policies) such as "connection speed." EX-1004, [0077]. A POSA evaluating Limont would recognize that Limont's advantage of updating policies using a server to a client is replicated by Polson's client gateway which provides additional devices (and device types) for Limont's corporate

administrators to effectuate the desire to control data usage and policy enforcement for traveling users. EX-1003, ¶¶624-629.

Based on their complementary capabilities in managing, enforcing and updating policies for traveling users (including corporate users), a POSA recognized the benefits of including Polson's teaching of a portable WWAN gateway as one of the managed mobile devices managed by Limont's network servers. EX-1003, ¶¶630.

Moreover, a POSA would have had a reasonable expectation of success in the combination. EX-1003, ¶¶631-639. Limont's managed devices need the capabilities to: (1) communicate with network servers; (2) receive updated policies; and (3) enforce those policies. Polson's gateway already performs all three functions using the same basic components (processor, memory, WLAN/WWAN interfaces) that implement Limont's managed client devices. EX-1003, ¶¶632-633.

The presence of Wright (and optionally Xu) does not impact the combination with Polson. EX-1003, ¶¶633-638, 165-222. Like Wright, Polson uses encryption on its various interfaces. EX-1008, Fig. 13 (encryption on WiFi interface). Polson and Wright (and Xu) describe compatible devices with computing and storage capabilities which would facilitate storage of any network

access information and policies in encrypted and/or secure memory as detailed in Wright and Xu. EX-1003, ¶¶633-638, 165-222.

3. Detailed Application to the Challenged Claims

a. Claims 3-5 "*The method of claim 1, wherein the wireless end-user device is an intermediate networking device…*

Claims 3-5 recite the requirement that the end-user devices is an *intermediate network device*. The '042 Patent distinguishes the claimed ""intermediate networking devices" as being different from "mobile communications devices" such as a "mobile phone."

> a communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways, …, and other intermediate network devices, **or** a mobile communications device, such as a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, a home networking system, and/or any other mobile communications device)

EX-1001, 5:41-50. The "**or**" clearly delineates between an "intermediate networking device" (as recited in these claims) and "mobile communication device[s]." EX-1003, ¶¶672-675. Thus, if PO attempts to restrict the term "intermediate networking device" to any specific device format (*e.g.*, "mobile phone"), such a construction conflicts with the '042 Patent and would be incorrect.

Moreover, by 2009, it was well-known to a POSA that such WLAN gateways (as Polson's) for forwarding traffic between WLAN and WWAN could be implemented in the form / size factor of a mobile phone or laptop. EX-1003, ¶¶223-254 (citing and discussing EX-1017, EX-1018, EX-1019, EX-1020).

[3.0] … for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).

Polson teaches a WWAN / WLAN gateway that meets this claim. EX-1003, ¶¶643-667. The '042 Patent identifies "gateways" as "intermediate network device." "[A] communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways …." EX-1001, 5:41-43; EX-1003 ¶¶643-646.

Polson's "gateway" is "any computing device capable of" forwarding data between WWAN / WLAN networks. Polson depicts the gateway in Figure 1:

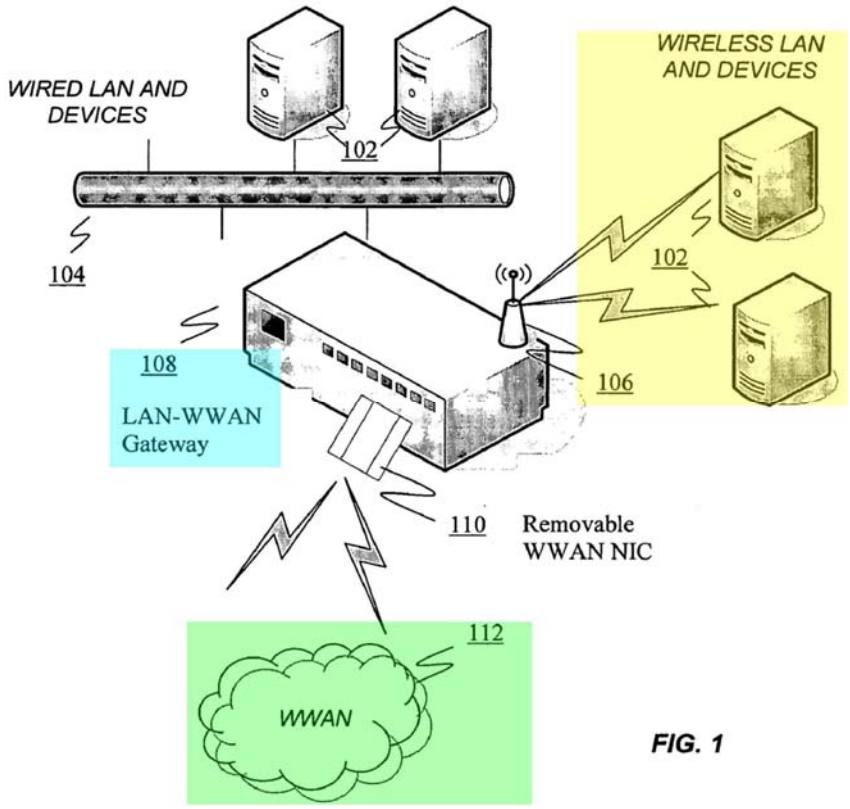


FIG. 1

EX-1008, Fig. 1 (annotated). The gateway connects to "wired" and "wireless" LANs interfaces and WWAN interfaces. EX-1008, [0020]; EX-1003 ¶¶648-649.

Polson's gateway forwards (routes) data between the WWAN and WLAN based on the user's subscription policies:

> [T]he routing engine of gateway 108 may facilitate two-way transmission of data to and from the one or more LANs and to and from one or more WWANs. As mentioned above, capabilities of the routing engine may be affected by the results of the subscriber determination logic. That is, receipt from and transmission to a WWAN may be based on a service agreement between a user and a wireless service provider.

EX-1008, [0039].

For example, data received from the WWAN can be forwarded to the recipient device on the WLAN:

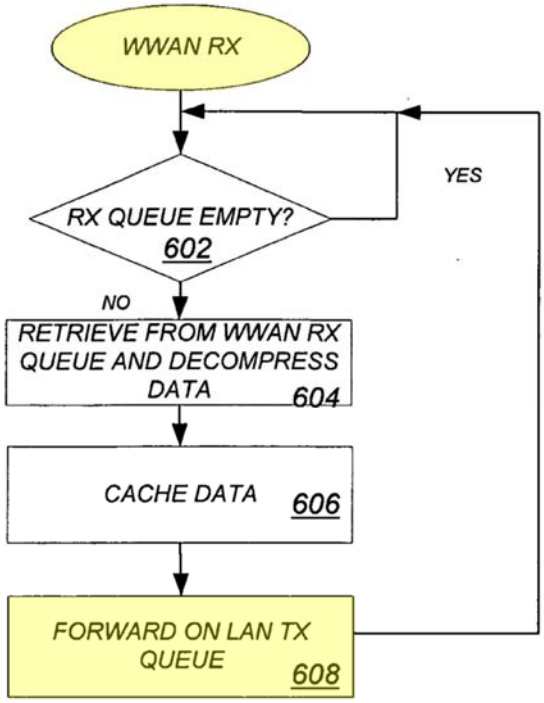


FIG. 6

EX-1008, Fig. 6; [0070-0073]. EX-1003, ¶¶647-655.

Figure 4 depicts the analogous operation when the gateway receives data from the LAN, determines to which network the data is addresses and forwards the LAN RX data to the WWAN TX queue.

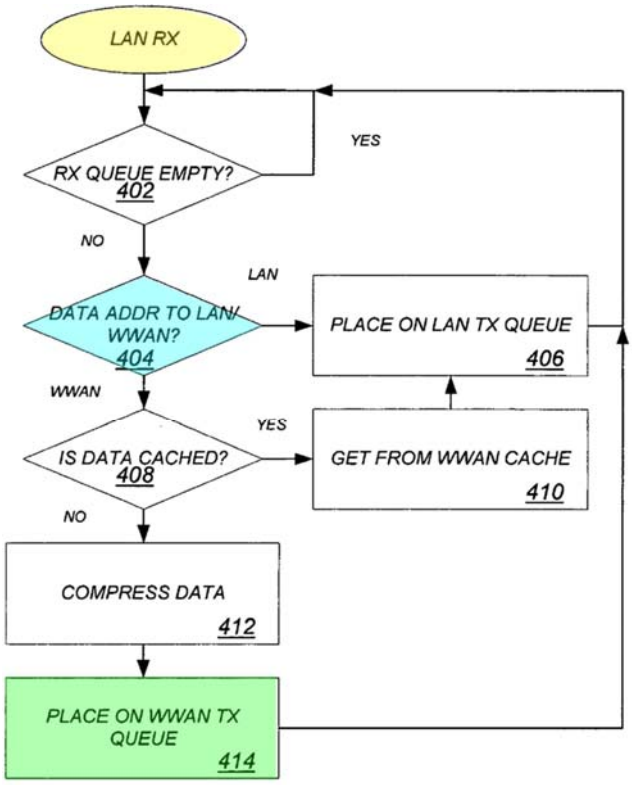


FIG. 4

EX-1008, Fig. 4; [0063-0067]. EX-1003, ¶¶647-661.

Limont identifies that "intermediate network devices" can exist on communication link 132 or 133 between an end-user device and servers. EX-1004, [0043], [0056]. Polson's "gateway" devices correspond to Limont's intermediate network devices and provide additional security by allowing Limont's server to control the policies on those intermediate network devices (Polson's gateways) and the devices attached to those gateways using the WLAN interfaces. EX-1003, ¶¶662-666.

Thus, in one proposed combination, Polson's gateway would be placed on link 132 and allow mobile device 101 to use the WLAN interface and forward data

to the WWAN interface toward the server. Similarly, Limont's policy settings include Polson's policies. EX-1003, ¶666.

b. Claim 4

[4.0] … comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network.

Polson discloses the claimed "intermediate networking device for forwarding" as "cellular device" as detailed for claim 3. The WWAN may be "cellular." EX-1008, [0051] ("The WWAN interface 110 may be … cellular, PCS, and WiMax WWAN interfaces."); [0054-0056], [0005]. EX-1003, ¶¶669-676.

c. Claim 5

[5.0] … and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.

Polson's gateway is an *intermediate networking device*. *See* claim 3. Polson teaches several policy settings that assist other end-user devices in communicating over the wireless access networks (both WLAN and WWAN). EX-1003, ¶¶678-695.

Polson's WWAN gateway includes "subscriber determination logic" applied to the devices and networks to which the gateway connects. EX-1008, [0029-0040]. The forwarding of data depends on the "service agreement" as implemented by the policies in the gateway. EX-1008, [0039].

Polson teaches switching between WWAN interfaces based "a different WWAN interface is stronger, or where the provider associated with the current WWAN interface 110 does not provide service." EX-1008, [0052]. Polson's WWAN switching mirrors Limont's described functionality of evaluating the "connection speed" and potentially updating the policies (such as the "network interface settings [and] wireless protocol settings") to use a new network providing the required connection speed and performs the "assist" in this claim. EX-1003, ¶¶682-687.

Another "assist" policy is that the "LAN 104 users may be authenticated onto the gateway … for WWAN 112 access…." EX-1008, [0035]. By "authenticating" the LAN users to allow for "WWAN access," the policy settings "assists" other end-user devices (the LAN users) in communicating over the WWAN as claimed and as taught in Limont. EX-1003, ¶¶688-691.

Polson's identifies additional policies that assist other end-user devices in accessing the WWAN including:

- the gateway will "allow" (or restrict) use of the WWAN "according to the [subscriber's] service agreement and/or the policies of the wireless service provider" including "quality of service …, the throughput provided, the cumulative bits per hour, day or month, port-forwarding, on-board VPN…." EX-1008, [0029-0030];

- specifying access for "certain period of time, a certain quantity of bytes downloaded, etc." or a particular number or type of device or a particular IP address. EX-1008, [0031-0032];
- Policies allowing specific access (*e.g.*, "unrestricted and restricted" access) to different aspects ("Access Point Name") on a cellular network ("GSM.") EX-1008, [0033];
- Policies allowing access based on the SIM, MIN or ESSID. EX-1008, [0034];
- Policies that "coordinate the wired and wireless access" for subscribers where "such coordination of wired and wireless access may be a feature of the service agreement, such as, for example, simultaneous wired and wireless access to maximize throughput for a premium service agreement" or the ability to have a "wireless preference" for access. EX-1008, [0036]
- "Customizable" policies to better the "overall user experience" including specific "customization may be implemented by a wireless service provider for a certain customer, for example for a large corporate customer of the wireless service provider." EX-1008, [0037].
- Policies that allow end-users to switch between different WWAN providers (networks) based on user preferences for access. EX-1008, [0038].

Each of these policies programmed into, and implemented by, Polson's gateway assists other users (for example, the LAN users) in communicating over the WWAN by, for example, allowing for access and specifying the contours of such access. EX-1003, ¶¶692-693. Moreover, Limont also specifically identifies such policies to be programmed into the client devices, such as Polson's gateway, as detailed in Ground 1 above. EX-1004, [0073], EX-1003, ¶¶693, 695.

VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION AND DENY INSTITUTION

A. The Board Should Not Deny Institution Under 35 U.S.C. § 325

Limont, Xu and Polson have not been considered by an Examiner or the Board against the Challenged Claims. Although Wright (as issued) was submitted by the applicant with over 1000 prior art references, the Examiner did not apply or discuss Wright. The claims were allowed in a first office action allowance without substantive comment. Because this Petition presents combinations of prior art and arguments that were not previously considered, the Board should not discretionarily deny institution under these circumstances.

B. The Board Should Not Deny Institution Under 35 U.S.C.§ 314(a)

The Board has discretion to deny institution under 35 U.S.C. § 314(a). Related to the Director's June 2022 interim guidance regarding application of the *Fintiv* factors[3], (1) the Petition is particularly strong in the underlying merits, and (2) Petitioners will not pursue in the Related Litigation any ground raised in this IPR. Thus, under the Interim Guidance, the Board should not deny institution.

[3] Interim Procedure For Discretionary Denials In AIA Post Grant Proceedings With Parallel District Court Litigation, PTO Director's Memorandum (June 21, 2022).

Nevertheless, the Board's decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed.

Under factor 2, trial date has been set for May 19, 2025. EX-1022. A Final Written Decision is expected in the present matter in November 2025. Considering the uncertainties of litigation scheduling, particularly as here where multiple trials are scheduled for the same date, this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties have not exchanged proposed claim terms or constructions, and will not complete claim construction briefing until September 2024. The Markman hearing is not until November 2024. Fact discovery is not set to close until December 2024, and expert discovery is not set to close until February 2025.; *See PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (finding that since no claim construction hearing had yet been held and discovery was not completed, the little investment in the parallel proceeding weighed against discretionary denial). Thus, this factor weighs against discretionary denial.

Under factor 4, there will not be complete overlap in the issues raised in the IPR and the Related Litigation and this favors institution. The Related Litigations

do not involve claims 10, 11, and 15 challenged herein. Also, PO asserted *300+* claims from four patents in the Related Litigations (EX-1021) – an amount that far exceeds the number of claims that the district court will allow at trial. See https://txed.uscourts.gov/?q=model-order-focusing-patent-claims-and-prior-art-reduce-costs. (Model Order limiting patentees to a "Final Election of Asserted Claims, which shall identify no more than five asserted claims per patent … and no more than a total of 16 claims"). Thus, it is highly unlikely the district court addresses the validity of even all 15 asserted claims of the '042.

Under factor 5, Petitioners are defendants in the Related Litigations. This factor is neutral as it is "far from an unusual circumstance that a petitioner in inter partes review and a defendant in a parallel district court proceeding are the same." *See Sand Revolution II LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 12-13 (PTAB June 16, 2020).

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are particularly strong and the claims did not receive any analysis during prosecution. For example, Limont is directed at the same problem and proposes the same solution as the '042 Patent, and discloses identical architecture and the identical concepts disclosed in the '042 Patent, thus demonstrating that the Petition is particularly strong in the merits.

When viewed holistically, the timing of the present Petition is reasonable, there has been relatively limited investment in the Related Litigation, and there is minimal overlap between the present IPR and the Related Litigation. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

VIII. Mandatory Notices Under 37 C.F.R. §42.8

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest in this Petition is Cellco Partnership d/b/a Verizon Wireless, Verizon Corporate Services Group Inc., T-Mobile USA, Inc., AT&T Services, Inc., AT&T Mobility LLC, and AT&T Corp..[4]

[4] Out of an abundance of caution, Petitioners identify all current defendants in the below identified cases as potential real parties in interest only for the purpose of this proceeding and only to the extent that Patent Owner contends that these separate legal entities should be named real parties in interest in this IPR. Petitioners do so to avoid the potential expenditure of resources to resolve such a challenge. Petitioners also acknowledge that each petitioner has a number of affiliates. No unnamed entity is funding, controlling, or otherwise has an opportunity to control or direct this Petition or Petitioner's participation in any

B. Related Matters (37 C.F.R. § 42.8(b)(2))

1. Judicial Matters

As of the filing date of this Petition and to the best knowledge of Petitioners, the '042 Patent is involved in the following litigations (the "Related Litigations"):

- *Headwater Research LLC v Verizon Communications Inc*., *et al*, Case No. 2:23-cv-00352-JRG-RSP (EDTX);
- *Headwater Research LLC v AT&T Inc.*, *et al,* Case No. 2:23-cv-00398-JRG-RSP (EDTX);
- *Headwater Research LLC v T-Mobile US, Inc., et al*, Case No. 2:23-cv-00379-JRG-RSP (EDTX);

Administrative Matters:

As of the filing date of this Petition and to the best knowledge of, the '042 Patent has not been subject to any Petitions for *inter partes* reviews.

2. Related Patents

See Exhibit 1023.

C. Lead/Back-up Counsel (37 C.F.R. § 42.8(b)(3)):

Lead Counsel:
Patrick D. McPherson, USPTO Reg. No. 46,255

resulting IPR. Petitioners are also not aware of any affiliate that would be barred from filing this Petition under 35 U.S.C. § 315(e).

DUANE MORRIS LLP

901 New York Avenue N.W., Suite 700 East

Washington, DC 20001

P: (202) 776-7800

F: (202) 776-7801;

PDMcPherson@duanemorris.com

Back-up Counsel:

Kevin P. Anderson, Reg. No. 43,471

DUANE MORRIS LLP

901 New York Avenue N.W., Suite 700 East

Washington, D.C. 20001

P: (202) 776-5213

F: (202) 776-7801

kpanderson@duanemorris.com

D. Notice of Service Information (37 C.F.R. § 42.8(b)(4)):

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioners consents to electronic service at the email addresses above.

IX. CONCLUSION

Petitioners have established a reasonable likelihood of prevailing on all Challenged Claims of the ’042 Patent and requests the Board institute *inter partes* review and then cancel all claims.

Respectfully submitted,

DUANE MORRIS LLP

BY: /Patrick D. McPherson/
Patrick D. McPherson
USPTO Reg. No. 46,255
Duane Morris LLP
505 9th Street NW, Suite 1000
Washington, D.C. 20004

Dated: April 19, 2024

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the April 19, 2024, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 9,198,042 and all supporting exhibits were served via Federal Express, postage prepaid, to the Patent Owner by serving the correspondence address of record for the '042 Patent:

106963 - Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA
UNITED STATES

With a courtesy copy to PO's litigation counsel at:

Reza Mirzaie (CA SBN 246953)
rmirzaie@raklaw.com
Neil Rubin (CA SBN)
nrubin@raklaw.com
Paul A. Kroeger (CA SBN 229074)
pkroeger@raklaw.com
Philip X. Wang (CA SBN 262239)
pwang@raklaw.com
James N. Pickens (CA SBN 307474)
jpickens@raklaw.com
Adam Hoffman
ahoffman@raklaw.com
Jacob Buczko
jbuczko@raklaw.com
Minna Chan
mchan@raklaw.com
Christian Conkle
cconkle@raklaw.com
RUSS AUGUST & KABAT
12424 Wilshire Blvd. 12th Floor

/Kevin P. Anderson/
Kevin P. Anderson
901 New York Avenue, N.W.,
Suite 700 East
P: (202) 776-7800
F: (202) 776-7801
KPAnderson@duanemorris.com

ATTORNEY FOR PETITIONERs

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq*., the undersigned certifies that this document complies with the type-volume limitations. This document contains 13,691 words as calculated by the "Word Count" feature of Microsoft Word 2010, the word processing program used to create it.

Dated: April 19, 2024

By: Kevin P. Anderson
Kevin P. Anderson,
Reg. No. 46,255
Duane Morris LLP
901 New York Avenue, N.W.,
Suite 700 East
Washington D.C., 20001
P: (202) 776-7800
F: (202) 776-7801
KPAnderson@duanemorris.com